



Calhoun: The NPS Institutional Archive DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2015-09

The role of North American Aerospace Defense Command (NORAD) in military cyber attack warning

DeGering, Randall R.

Monterey, California: Naval Postgraduate School

<http://hdl.handle.net/10945/47244>

Copyright is reserved by the copyright owner.

Downloaded from NPS Archive: Calhoun



<http://www.nps.edu/library>

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community.

Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

**Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943**



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**THE ROLE OF NORTH AMERICAN AEROSPACE
DEFENSE COMMAND (NORAD) IN MILITARY CYBER
ATTACK WARNING**

by

Randall R. DeGering

September 2015

Thesis Advisor:
Co-Advisor:

Rudy Darken
Ryan Ellis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 2015	3. REPORT TYPE AND DATES COVERED Master's Thesis
4. TITLE AND SUBTITLE THE ROLE OF NORTH AMERICAN AEROSPACE DEFENSE COMMAND (NORAD) IN MILITARY CYBER ATTACK WARNING		5. FUNDING NUMBERS
6. AUTHOR(S) DeGering, Randall R.		8. PERFORMING ORGANIZATION REPORT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		10. SPONSORING/MONITORING AGENCY REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number N/A .

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A
---	------------------------------------

13. ABSTRACT (maximum 200words)

For more than fifty years, North American Aerospace Defense Command (NORAD) has been responsible for conducting aerospace warning and control missions for the defense of North America. In accomplishing those operations, Commander NORAD is responsible for making the official warning to both the president of the United States and the prime minister of Canada if North America is suddenly under aerospace attack.

Now, with the dramatic increase in worldwide cyberspace events, NORAD has begun examining its own potential role within this new domain. Would involving NORAD in the military cyber attack warning process, leveraging its unique and proven binational structure, provide any advantages to both nations?

To analyze this question, this thesis briefly traces NORAD's warning mission history, discusses the basic concepts involved with "cyber attacks," identifies key U.S. and Canadian military cyber organizations, and examines significant U.S. and Canadian cyberspace government policies. It then proposes three potential new courses of action for NORAD, identifying advantages, disadvantages, and proposed solutions to implementation.

The thesis ends by recommending NORAD advocate for unrestricted cyberspace national event conference participation. This would be a realistic, achievable first step offering significant improvement in both NORAD's cyber attack situational awareness, as well as improving overall operational responsiveness.

14. SUBJECT TERMS NORAD, U.S. Cyber Command, cyber event, cyber attack warning, cyberspace domain, cyber threat actors, cyberweapons, defensive cyberspace operations, cyber watch conference		15. NUMBER OF PAGES 107
16. PRICE CODE		
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified
		20. LIMITATION OF ABSTRACT UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**THE ROLE OF NORTH AMERICAN AEROSPACE DEFENSE COMMAND
(NORAD) IN MILITARY CYBER ATTACK WARNING**

Randall R. DeGering
B.S., University of Maryland, 1982
M.A., University of Oklahoma, 1989

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2015**

Author: Randall R. DeGering

Approved by: Dr. Rudy Darken
Thesis Advisor

Dr. Ryan Ellis
Co-Advisor

Dr. Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

For more than fifty years, North American Aerospace Defense Command (NORAD) has been responsible for conducting aerospace warning and control missions for the defense of North America. In accomplishing those operations, Commander NORAD is responsible for making the official warning to both the president of the United States and the prime minister of Canada if North America is suddenly under aerospace attack.

Now, with the dramatic increase in worldwide cyberspace events, NORAD has begun examining its own potential role within this new domain. Would involving NORAD in the military cyber attack warning process, leveraging its unique and proven binational structure, provide any advantages to both nations?

To analyze this question, this thesis briefly traces NORAD's warning mission history, discusses the basic concepts involved with "cyber attacks," identifies key U.S. and Canadian military cyber organizations, and examines significant U.S. and Canadian cyberspace government policies. It then proposes three potential new courses of action for NORAD, identifying advantages, disadvantages, and proposed solutions to implementation.

The thesis ends by recommending NORAD advocate for unrestricted cyberspace national event conference participation. This would be a realistic, achievable first step offering significant improvement in both NORAD's cyber attack situational awareness, as well as improving overall operational responsiveness.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	SCOPE AND METHODOLOGY	2
C.	THESIS OUTLINE.....	3
II.	OPERATIONAL OVERVIEW	5
A.	INTRODUCTION.....	5
B.	TRADITIONAL NORAD WARNING MISSIONS	5
1.	Early North American Air Defense Warning	5
2.	Intercontinental Ballistic Missile Warning.....	8
3.	Cruise Missile Warning.....	11
4.	Cooperation with USNORTHCOM	12
C.	NORAD'S NEW MARITIME WARNING MISSION	13
D.	THE FUTURE OF NORAD?	14
E.	CYBER WARFARE COMPONENTS	16
1.	Current Cyberspace Threat Actors	16
2.	Typical Cyber Weapons	18
3.	Concept of “Cyber Attack”	19
4.	Military Cyberspace Definitions.....	24
F.	KEY U.S. MILITARY CYBER ORGANIZATIONS	27
1.	Department of Defense	27
2.	Joint Chief of Staff	27
3.	U.S. Northern Command	29
4.	U.S. Strategic Command	30
5.	U.S. Cyber Command.....	31
G.	KEY CANADIAN MILITARY CYBER ORGANIZATIONS	32
1.	Department of National Defence	32
2.	Strategic Joint Staff	33
3.	Canadian Joint Operations Command	34
4.	Canadian Forces Information Operations Group	35
H.	MILITARY CYBER EVENT CONFERENCES.....	36
1.	Cyber Event Conferences.....	36
2.	National Event Conference	37
I.	SUMMARY	40
III.	LITERATURE REVIEW	41
A.	INTRODUCTION.....	41
B.	NORAD GUIDANCE	41
1.	NORAD Agreement.....	41
2.	NORAD Strategic Review	43
C.	U.S. NATIONAL CYBERSPACE GUIDANCE	44
1.	Executive Branch	44
a.	<i>National Strategy to Secure Cyberspace (2003)</i>	44

<i>b.</i>	<i>Comprehensive National Cybersecurity Initiative (2008)</i>	44
<i>c.</i>	<i>Cyberspace Policy Review (2009).....</i>	45
<i>d.</i>	<i>National Security Strategy (2010)</i>	46
<i>e.</i>	<i>U.S. International Strategy for Cyberspace (2011)</i>	46
<i>f.</i>	<i>PPD-20, U.S. Cyber Operations Policy (2012)</i>	47
2.	Department of Defense	48
<i>a.</i>	<i>National Military Strategy for Cyberspace Operations (2006).....</i>	48
<i>b.</i>	<i>Unified Command Plan (2011).....</i>	48
<i>c.</i>	<i>National Military Strategy (2011).....</i>	49
<i>d.</i>	<i>CJCS Volume VI Emergency Action Procedures (2012).....</i>	50
<i>e.</i>	<i>Joint Publication 3-12, Cyberspace Operations (2013)</i>	50
D.	CANADIAN NATIONAL CYBERSPACE GUIDANCE	51
1.	Executive Branch	51
<i>a.</i>	<i>Canada's Cyber Security Strategy (2010)</i>	51
<i>b.</i>	<i>Action Plan 2010–2015 (2013)</i>	51
2.	Department of National Defence	52
<i>a.</i>	<i>Canada First Defence Strategy (2013).....</i>	52
<i>b.</i>	<i>Canadian Forces Cyber Operations Primer (2014).....</i>	52
E.	SUMMARY	52
IV.	COURSES OF ACTION DEVELOPMENT	55
A.	METHODOLOGY	55
B.	COA #1 DESCRIPTION (FULL NORAD CYBER CONFERENCE PARTICIPATION).....	56
1.	Definition	56
2.	Discussion.....	56
3.	Advantages.....	56
4.	Disadvantages and Proposed Solutions.....	57
C.	COA #2 DESCRIPTION (NORAD ALL-DOMAIN WARNING PRODUCTION).....	57
1.	Definition	57
2.	Discussion.....	57
3.	Advantages.....	58
4.	Disadvantages and Proposed Solutions.....	58
D.	COA #3 DESCRIPTION (JOINT NORAD + USCYBERCOM CYBER ATTACK ASSESSMENT).....	59
1.	Definition	59
2.	Discussion.....	59
3.	Advantages.....	59
4.	Disadvantages and Proposed Solutions.....	60
E.	SUMMARY	61
V.	COURSES OF ACTION ANALYSIS.....	63
A.	METHODOLOGY	63
B.	COA #1 ANALYSIS (FULL NORAD CYBER CONFERENCE PARTICIPATION).....	64

1.	Advantages, Disadvantages and Weighted Scoring.....	64
2.	COA #1 Synopsis.....	65
C.	COA #2 ANALYSIS (NORAD ALL-DOMAIN WARNING PRODUCTION).....	66
1.	Advantages, Disadvantages and Weighted Scoring.....	66
2.	COA #2 Synopsis.....	67
D.	COA #3 ANALYSIS (JOINT NORAD + USCYBERCOM CYBER ATTACK ASSESSMENT).....	68
1.	Advantages, Disadvantages and Weighted Scoring.....	68
2.	COA #3 Synopsis.....	70
E.	COA ANALYSIS COMPARISON.....	71
VI.	FINDINGS AND RECOMMENDATIONS	75
A.	FINDINGS	75
B.	RECOMMENDATIONS	78
LIST OF REFERENCES		79
INITIAL DISTRIBUTION LIST		85

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	North American Distant Early Warning (DEW) Site.....	6
Figure 2.	Original NORAD “Air” Emblem of 1958.....	7
Figure 3.	Thule BMEWS Site.....	8
Figure 4.	SBIRS Space-Based Warning Satellite.....	9
Figure 5.	New NORAD “Aerospace” Emblem of 1981.....	10
Figure 6.	AWACS Airborne Early Warning (AEW) Aircraft.....	11
Figure 7.	Headquarters NORAD and USNORTHCOM.....	12
Figure 8.	Maritime Threat Routes.....	13
Figure 9.	DOD Cyberspace Operations.....	26
Figure 10.	DOD Organizational Chart.....	28
Figure 11.	DOD and JCS Emblems.....	28
Figure 12.	USNORTHCOM Emblem.....	29
Figure 13.	USSTRATCOM Emblem.....	30
Figure 14.	USCYBERCOM Emblem.....	31
Figure 15.	DND Organizational Chart.....	33
Figure 16.	DND and SJS Crests.....	34
Figure 17.	CJOC Crest.....	35
Figure 18.	DGIMO, CFIOG and CFNOC Crests.....	36
Figure 19.	Cyber Event Conferences.....	38
Figure 20.	NORAD-USNORTHCOM Command Center.....	40

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Cyberspace Attack Assessment Criteria.....	38
Table 2.	COA #1 Scoring Summary.....	64
Table 3.	COA #2 Scoring Summary.....	67
Table 4.	COA #3 Scoring Summary.....	69
Table 5.	COA Analysis Summary.....	73

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AWACS	Airborne Warning and Control System
BMEWS	Ballistic Missile Early Warning System
BPG	Binational Planning Group
CAF	Canadian Armed Forces
CDS	Chief of Defence Staff (Canada)
CFEWC	Canadian Forces Electronic Warfare Centre
CFIOG	Canadian Forces Information Operations Group
CFNOC	Canadian Forces Network Operations Centre
CFS	Canadian Forces Station
CJCS	Chairman, Joint Chiefs of Staff (U.S.)
CJOC	Canadian Joint Operations Command
COA	Course of Action
CONAD	Continental Air Defense Command
DCO	Defensive Cyber Operations
DCO-RA	Defensive Cyber Operations-Response Actions
DND	Department of National Defence (Canada)
DOD	Department of Defense (U.S.)
DODIN	DOD Information Networks
DSOC	DOD Strategy for Operating in Cyberspace
EW	Electronic Warfare
ICBM	Intercontinental Ballistic Missile
IRGC	Iranian Revolutionary Guard Corps

JS	Joint Staff (U.S.)
MDA	Maritime Domain Awareness
MDMP	Military Decision Making Process
N2C2	NORAD and NORTHCOM Command Center
NATO	North Atlantic Treaty Organization
NEC	National Event Conference
NMS	National Military Strategy
NMS-CO	National Military Strategy-Cyberspace Operations
NSA	National Security Agency
OCO	Offensive Cyber Operations
OGPC	Operation GLADIATOR PHOENIX Conference
OSD	Office of the Secretary of Defense (U.S.)
PLA	People's Liberation Army
RCAF	Royal Canadian Air Force
SBIRS	Space-Based Infrared System
SCI	Special Compartmented Information
SecDef	Secretary of Defense (U.S.)
SJS	Strategic Joint Staff (Canada)
TTP	Tactics, Techniques, and Procedures
USAF	U.S. Air Force
UCP	Unified Command Plan

EXECUTIVE SUMMARY

Since 1958, North American Aerospace Defense Command (NORAD) has a proven history of adapting and evolving to meet changing military defense challenges using new technology—from its early years providing ground-based radar warning of approaching Soviet bombers, to ground-based radar warning of in-bound Soviet ICBMs, to satellite-based warning of any missile launch occurring around the world, to extended radar warning of approaching cruise missiles, to the warning of suspect maritime vessels approaching North America. Overall, NORAD has sole responsibility for receiving early warnings from numerous space-based and ground-based sensors and developing an integrated North American attack assessment.

Because all of the sensors feeding into NORAD travel across the broader “information superhighway,” there exists a genuine risk of potentially hostile nations conducting damaging cyberspace operations against NORAD (to include blinding NORAD to actual threats or feeding the Command false information for incorrect action.) With the recent increase in worldwide cyberspace events, NORAD has thus begun examining its own potential role in this new operational domain.

An exact definition regarding what constitutes a “cyber attack” remains in flux. Despite this lack of definition, however, both the U.S. and Canada have been quick to establish new, dedicated military organizations specializing in conducting cyberspace operations. Further, current military cyberspace event conferences now share warning information between U.S. Combatant Commands around the world, to include the NORAD and USNORTHCOM Command Center. (One area of concern: current U.S. classification policies restrict the sharing of certain classified information with Canadian NORAD members.)

Over the course of 50 years, NORAD has repeatedly reassessed, redefined, and updated its core operational missions based upon a constantly evolving threat. The NORAD Agreement clearly reflects both Nation’s desire that NORAD be able to adapt and defend against newly evolving military threats which each nation may jointly face.

Likewise, numerous U.S. and Canadian national strategies recommend working with international organizations to develop international watch-and-warning networks in order to detect and prevent cyber attacks. U.S. military policy encourages the necessity to integrate allies early in planning discussions in order to reduce operational boundaries, thus increasing the chances of success in combined operations. Finally, from a Canadian perspective, both Canada's civilian and military strategies mirror the same themes of working with international organizations to develop international watch-and-warning networks in order to detect and prevent cyber attacks.

With this background in mind, this thesis developed three courses of action (COAs) regarding possible roles NORAD might play in future military cyber attack warning situations. Each proposed COA was initially analyzed to ensure it met specific validity criteria (e.g., adequate, feasible, acceptable, distinguishable, and complete.) COAs were then arranged by increasing levels of responsibility being placed upon NORAD. Each COA was then examined for specific advantages, disadvantages, and possible solutions for successful implementation.

After considering these three COAs, this thesis proposes NORAD advocate for unrestricted national cyberspace event conference participation. This would seem to be a realistic, achievable first step that offers significant improvement in NORAD cyber attack situational awareness and improved operational responsiveness, while requiring only a change in DOD information classification policy for implementation. Allowing NORAD Canadian personnel to fully participate in real-time cyber event conferences would fulfill stated U.S. and Canadian national policies, which repeatedly highlight the need for greater cooperation and information sharing with between allies.

In conclusion, while requiring challenging staff actions nationally within DOD and internationally with Canada to provide unrestricted access to cyberspace operations, the recommended action harnesses proven NORAD binational relationships and warning procedures to provide all-domain warnings to both nations.

ACKNOWLEDGMENTS

I feel very fortunate to have been selected as the NORAD and USNORTHCOM nominee to attend this prominent program sponsored by the Naval Postgraduate School's Center for Homeland Defense and Security (CHDS).

I hope my research into the question of what role NORAD might play in any future military cyber attack warning mission for North America will help inform policy makers at NORAD-USNORTHCOM, USCYBERCOM, the U.S. Department of Defense (DOD), and the Canadian Department of National Defence (DND).

First, genuine thanks go to Dr. Rudy Darken and Dr. Ryan Ellis, my excellent co-advisors during the development of this thesis. Thanks also to Dr. Carolyn Halladay and Dr. Lauren Wollman, my research and writing advisors. Also, many thanks go to Dr. Chris Bellavita, our CHDS Academic Programs director and mentor throughout this entire master's degree process.

Next, sincere thanks go to my colleagues at NORAD and USNORTHCOM, for without their invaluable support and cyberspace expertise I could not have completed this thesis. This list includes Lt. Col. Joe Lawrence, Lt. Col. Sean Amutan, and Mark Clements of the N-NC/J52 Policy and Doctrine Division; Terry Boston of the N-NC/J53 Strategy Division; Lt. Col. Josh Zaker of the N-NC/J55 Plans Division; Kurt Danis and Robert Peterman of the N-NC/J63 Current Cyberspace Operations Division; Maj. Dragis Ivkovic (CF) and Frank Skinner of the N-NC/J65 Cyber Plans Division; and Maj. Daniel Gendreau (CF) of the N-NC/J85 Capabilities Integration Division.

Finally, a very special thanks to my wife, Janet, who continuously encouraged and supported me throughout this entire educational adventure.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

For more than fifty years, North American Aerospace Defense Command (NORAD) has been responsible for conducting aerospace warning and aerospace control for North America. These two aerospace missions involve the combined efforts of military forces of both the U.S. and Canada to detect airborne threats approaching or flying within North America (aerospace warning), and then taking appropriate actions to determine the aircraft of interest's actual intentions (aerospace control). The commander of NORAD is responsible for making an official assessment to the president and the Canadian prime minister if North America is under aerospace attack.

Similarly, U.S. Cyber Command (USCYBERCOM) is responsible for defending the U.S. military's cyberspace enterprise. The commander of USCYBERCOM is responsible for making an official assessment to the president if the U.S. military is under cyber attack. Would involving NORAD in the military cyber attack assessment process, leveraging its unique and proven binational structure, provide any advantages?

This thesis explores a new NORAD role in cyberspace defense, which is not one of its legacy air defense missions. However, there exists precedence for adding a new, non-aerospace related mission to NORAD; that being, the addition of the Maritime Warning mission to NORAD in 2006.

With cyber attacks by nation-states on the rise, this thesis investigates if there is an advantage in involving the assessment of military cyber attacks with a binational military command. Potential advantages may include operational efficiencies, improved cyberspace defense readiness, and/or enhanced situational awareness of a precursor cyberspace attack before any kinetic attack upon North America. Disadvantages may involve difficulties sharing cyberspace defense information between U.S. and Canadian cyberspace defense agencies, or an actual lessening of operational effectiveness of USCYBERCOM cyberspace defense operations themselves.

B. SCOPE AND METHODOLOGY

This thesis specifically focuses on the military cyberspace enterprise, and how NORAD and the individual military organizations of both the U.S. and Canada might jointly conduct military cyber attack warning. Therefore, no review was conducted of civilian cyberspace-related policies or strategies published by either by the U.S. Department of Homeland Security (DHS) or Department of Justice (DOJ), or by Canada's Public Safety (PS) Canada.

This problem statement also does not propose having NORAD assume the technical cyberspace defensive/offensive functions performed by USCYBERCOM. The thesis simply asks, "What is NORAD's role when assessing whether the U.S.' and/or Canada's military are under a military-related cyber attack?"

The question of whether NORAD should play a role in cyber attack warning does not seem to have been investigated previously. A literature review identifying the significant national cyberspace policies for both the U.S. and Canada has been accomplished, as well as a review of the key military strategies for cyberspace published by both countries. Literature outlining strategic cyberspace policies and general strategies of both the U.S. and Canada are well defined and unclassified. Military doctrine regarding cyberspace operations is also available, but details become classified as discussions become more technically oriented.

Every five years, NORAD conducts an internal self-assessment to determine if the Command is accomplishing the right missions, using the right approaches. Recently the headquarters staff began its investigation regarding NORAD's role in cyberspace defense, and expressed great interest and willingness to support this research. This thesis used existing documentation as well as dialogue with Headquarters NORAD and USNORTHCOM, USCYBERCOM, and Canadian military cyberspace practitioners.

This thesis then developed three courses of action, and outlined their advantages and disadvantages. It then proposed solutions for each disadvantage, and weighted the difficulty of implementing each solution. For each course of action, a numerical score was then assigned. The lowest score indicated an option potentially easier to implement, while a high scoring option was potentially more difficult.

Overall, the cyber warning topic is important, valuable, relevant, and enduring. The eventual goal is to present this completed thesis to the NORAD Strategy and Policy Division for subsequent staff action.

C. THESIS OUTLINE

Chapter II opens with an operational overview, beginning with a short history of NORAD's evolving warning missions. The chapter then discusses cyber warfare components and includes a discussion regarding the difficulty of defining what is meant by a "cyber attack." Next, the chapter lists key U.S. and Canada military organizations involved in national cyberspace operations. The chapter closes with a review of differing military cyber event conferences.

Chapter III reviews current NORAD, U.S., and Canadian military policy regarding cyberspace operations, providing the reader numerous examples of national strategic guidance directing greater cooperation between both nations.

Chapter IV lays out three proposed courses of action (COA) for NORAD, from removing classification barriers to allow better information sharing, to fusing and disseminating all-domain threat warnings to both nations, to jointly participating with U.S. Cyber Command in assessing actual cyber attacks. Each COA is then examined for advantages, disadvantages, and proposed solutions for implementation.

Chapter V then analyzes each COA using a weighted scoring methodology to determine the relative difficulty in implementing each course of action. A lower score indicated an option potentially easier to implement, while a higher scoring option was potentially more difficult.

Chapter VI concludes with the overall findings and a recommendation.

THIS PAGE INTENTIONALLY LEFT BLANK

II. OPERATIONAL OVERVIEW

A. INTRODUCTION

In order to consider what role NORAD might play in military cyber attack warnings, we first need a general understanding of several fundamental topics. This chapter will briefly review the history of NORAD and its evolving military warning missions. Next, cyber warfare components and several proposed definitions for what a “cyber attack” might actually involve will be reviewed. Then, key U.S. and Canada military organizations involved in military cyber warfare will be highlighted. Finally, the chapter closes with a review of current military cyberspace attack conferences and the military cyberspace attack assessment process.

B. TRADITIONAL NORAD WARNING MISSIONS

1. Early North American Air Defense Warning

With the beginning of the Cold War during the late 1940s, American defense experts began planning a new, comprehensive air defense strategy they believed was critical in defending the U.S. against attacks by long-range Soviet Union strategic bombers. Led by the U.S. Air Force’s newly established “Air Defense Command” (created in 1948), regional commands were charged with protecting various areas of the U.S. from bomber attacks.¹

In August 1949, the Soviet Union detonated its first atomic bomb under project “First Lighting.”² The test shocked the Western powers, as the American intelligence community had previously estimated the Soviets would not develop an atomic weapon until 1953, at the very earliest.³ It was now predicted the Soviet Union would soon have the means to drop atomic weapons on the U.S. using long-range strategic bombers.

¹ NORAD History Office, Brief History of NORAD, (Colorado Springs, CO: 31 Dec 2012).

² Carey Sublette, “The Soviet Nuclear Weapons Program,” *The Nuclear Weapons Archive*, last modified 12 December 2007, <http://nuclearweaponarchive.org/Russia/Sovwpnprog.html>.

³ Ibid.

Thus, as concerns about Soviet nuclear capabilities became dire, in 1954 the Department of Defense formed a new, multi-service command called “Continental Air Defense Command” (CONAD) involving Army, Naval, and Air Force forces. As their service contribution, the Air Force provided interceptor fighter aircraft and agreed to operate an extensive array of arctic distant early warning radar sites which would act as a “trip wire” against any surprise Soviet bomber attack launched over the North Pole.

In addition, new defense agreements between Canada and the United States were negotiated, centering on building three series of long-range ground radar warning sites across Canada—the southern “Pinetree Line,” the “Mid-Canada Line,” and the famous northern “Distant Early Warning (DEW) Line.” (See Figure 1.)



Figure 1. North American Distant Early Warning (DEW) Site.⁴

⁴ Tom Page, “Alaskan DEW Line Sites,” *Radomes, Inc.*, accessed 20 Apr 2015, <http://www.radomes.org/museum/alaskadew.php>.

Based upon the remarkable success of these joint United States-Canadian radar construction efforts, in late 1957, the U.S. and Canada then jointly agreed to create an innovative “North American Air Defense Command” (NORAD), merging the operational control of both United States and Canadian air defense forces under a single, multinational military command.

NORAD was officially established on 12 May 1958.⁵ (See Figure 2.)



Figure 2. Original NORAD “Air” Emblem of 1958.⁶

The two nations formalized this mutual air defense arrangement in a new, binational defense agreement to be known as the “NORAD Agreement.” The NORAD Agreement, with its requirement for periodic review every five years, ensured the United States and Canada the flexibility to adapt the new Command to any changes in the defense environment over the coming years.

⁵ NORAD History Office.

⁶ Ibid.

2. Intercontinental Ballistic Missile Warning

Adding to the continental defense challenge, Soviet engineers soon developed a new intercontinental ballistic missile (ICBM) capable of delivering small, newly developed hydrogen bomb warheads. Thus, long range missile attacks now became a critical defense problem, as NORAD's vast line of arctic air defense radar sites could now "not only [be] outflanked, but literally jumped over."⁷

In response to this major ICBM threat, beginning in 1959, the Ballistic Missile Early Warning System (BMEWS) was developed (see Figure 3). Consisting of huge 165 feet high by 400 feet long radars, BMEWS became the first operational ballistic missile detection and warning system, designed to provide 15–25 minutes critical warning of a Soviet missile attack launched directly over the North Pole.



Figure 3. Thule BMEWS Site.⁸

⁷ *Brief History of NORAD*, 6.

⁸ Tom Page, "BMEWS Site 1, Under Construction - 1958–1960," *Radomes, Inc.*, accessed 19 Feb 2014, <http://radomes.org/museum/documents/BMEWSSite1ThuleGL1958-60construction.html>.

Later, because of growing concerns these BMEWS radars were unable to observe actual Soviet launches occurring far beyond the Earth's horizon, the U.S. began developing its own missile technology to orbit successive generations of early warning satellites capable of immediately detecting any ICBM launch occurring around the globe.

Space-based early warning progressed from the nascent "Missile Defense Alarm System" (MIDAS) system developed in the 1960s, to the more capable "Defense Support Program" (DSP) series of satellites employed during the 1970s to 1990s, to the current "Space-Based Infrared System" (SBIRS) series of satellites first launched in the 2000s. (See Figure 4.)

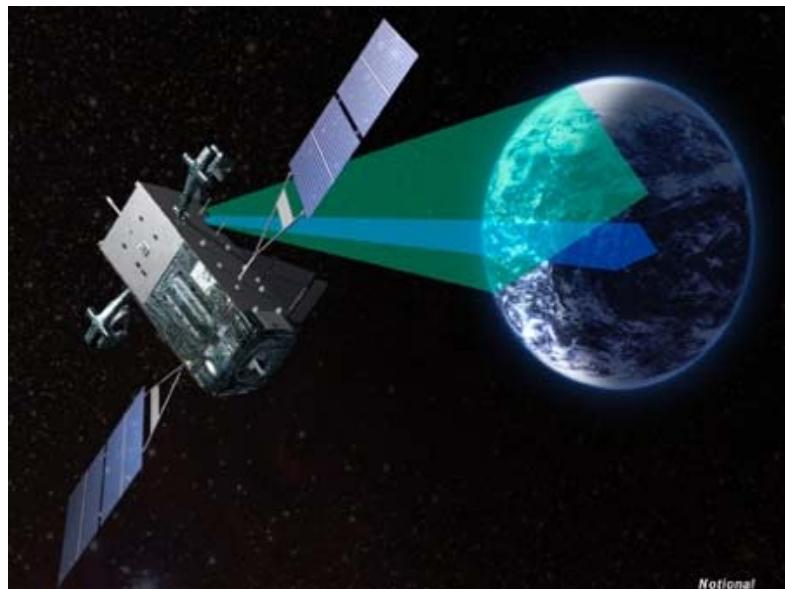


Figure 4. SBIRS Space-Based Warning Satellite⁹

⁹ Lockheed Martin Corp, "Space-Based Infrared System (SBIRS)," accessed 19 Dec 2014, <http://www.lockheedmartin.com/us/products/sbirs.html>.

Operating from geostationary orbit over 22,000 miles above the earth, these early warning satellite systems were designed to immediately detect any missile launches or nuclear explosions occurring across the globe using sensitive on-board sensors which could detect the infrared emissions from such intense heat sources.¹⁰

Thus, an evolving Soviet threat caused NORAD to adapt its warning missions to include both aircraft and missile attacks on North America. Reflecting that evolution, the 1981 NORAD Agreement officially changed the command's name to the North American "Aerospace" Defense Command. (See Figure 5.)



Figure 5. New NORAD "Aerospace" Emblem of 1981.¹¹

¹⁰ U.S. Air Force Factsheet, "Infrared Satellites," accessed 19 Dec 2014, <http://www.la.af.mil/library/factsheets/factsheet.asp?id=20144>.

¹¹ NORAD History Office.

3. Cruise Missile Warning

While ICBMs remained the preferred weapons for attacking strategic land targets, beginning in the 1970s, both the U.S. and the Soviet Union began developing new subsonic air-launched cruise missiles as a means of increasing the effectiveness of their strategic bomber force, while complicating the air defenses used by the enemy.¹²

To meet this new threat, beginning in the 1980s, NORAD air defense plans began calling for the use of newly developed USAF Airborne Warning and Control System (AWACS) radar aircraft. Using airborne platforms allowed NORAD to greatly extend its ground-based radar surveillance coverage, thus enabling it to detect and warn against enemy cruise missiles approaching the coast of North America. (See Figure 6.)



Figure 6. AWACS Airborne Early Warning (AEW) Aircraft¹³

¹² Federation of American Scientists, “Cruise Missiles,” accessed on 3 Apr 2015, <http://fas.org/nuke/intro/cm/index.html>.

¹³ <http://www.globalsecurity.org/military/systems/aircraft/images/Awacs3-onw.jpg>. Accessed 21 Apr 2015.

4. Cooperation with USNORTHCOM

The attacks on 11 September 2001 made it clear assaults on the homeland could now arrive from within a nation's borders. Thus, in October 2002, the U.S. Department of Defense (DOD) stood up its new U.S. Northern Command (USNORTHCOM), a joint military command specially tasked to execute the homeland defense mission.¹⁴ With NORAD executing the continental air defense mission, it seemed reasonable to co-locate the new USNORTHCOM headquarters with NORAD in Colorado Springs, and adopt a dual-hatted commander relationship.¹⁵ (See Figure 7.)



Figure 7. Headquarters NORAD and USNORTHCOM.¹⁶

¹⁴ U.S. Northern Command, "About USNORTHCOM," accessed 3 Apr 2015, <http://www.northcom.mil/AboutUSNORTHCOM.aspx>.

¹⁵ Ibid.

¹⁶ http://static.progressivemediagroup.com/uploads/imagelibrary/NORADheadquarters_2006_b.jpg. Accessed 21 Apr 2015.

C. NORAD'S NEW MARITIME WARNING MISSION

As an aftermath of the 9/11 attacks, Canada and the U.S. created a Binational Planning Group (BPG) in 2004 to work on multiple proposals for creating wider cooperation between Canadian and U.S. military plans and protocols, and to look for common mission areas in which the two countries could share information. One area of mutual interest was improving awareness of maritime threat routes which surround the North American continent.¹⁷ (See Figure 8.)

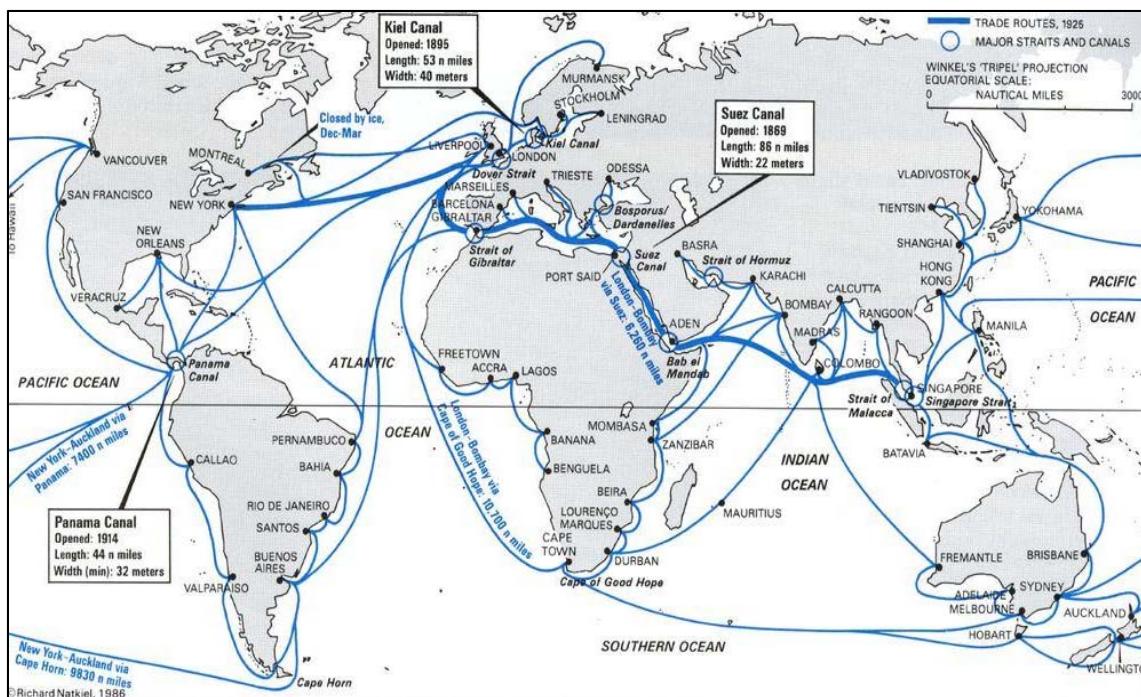


Figure 8. Maritime Threat Routes.

¹⁷ “2014: Piracy, Terrorism and Direct Maritime Threats,” *The Maritime Executive*, 14 Mar 2014, accessed 20 Apr 2015, <http://www.maritime-executive.com/article/2014-Piracy-Terrorism--Diverse-Maritime-Threats-2014-03-14>.

In a letter to the Chairman of the Joint Chiefs of Staff, Commander NORAD supported the concept of NORAD being tasked with a new maritime surveillance, warning, and information sharing mission.¹⁸

Thus, after lengthy staffing actions between headquarters, the U.S. and Canada signed a renewed NORAD Agreement, effective 12 May 2006, assigning NORAD with its new Maritime Warning mission, formally defined as:

c. Maritime warning consists of processing, assessing, and disseminating intelligence and information related to the respective maritime areas and internal waterways of, and the maritime approaches to, the U.S. and Canada, and warning of maritime threats to, or attacks against North America utilizing mutual support arrangements with other commands and agencies, to enable identification, validation, and response by national commands and agencies responsible for maritime defense and security.¹⁹

D. THE FUTURE OF NORAD?

In 2012, both the U.S. Chairman of the Joint Chiefs of Staff (CJCS) and the Canadian Chief of Defense Staff (CDS) jointly directed Commander NORAD to conduct a “NORAD Strategic Review” to address the following specific issues:

- Review current and potential future roles, missions, and command relationships.
- Inform and support analysis of need for investment in NORAD capabilities.
- Recommend linkages to align respective national research and development, planning, programming and budgeting processes related to NORAD requirements.
- Recommend ways to align readiness reporting processes.²⁰

¹⁸ NORAD History Office, Letter from CDRNORAD to CJCS, dated 15 Jul 2004.

¹⁹ NORAD History Office, *NORAD Agreement*, 28 Apr 2006.

²⁰ NORAD and USNORTHCOM, *NORAD Strategic Review*, 3 Dec 2014. (Note: Only unclassified paragraphs were quoted.)

When asked about the pending NORAD Strategic Review, General Charles Jacoby (then-Commander NORAD) replied:

We are deliberately moving out on a review that looks at the threat assessment, readiness assessment and program assessment processes that we need to put in place or revitalize, as the case may be, to ensure that we're staying ahead of the threat. The threat to North America is changing and increasing as time goes by, *and that includes cyber threats*, threats to space, changing in the extremist threat to North America, changing in some of the more conventional threats and making sure that NORAD is positioned to keep faith with the agreement. (Emphasis added)²¹

Completed in November 2014, the Review “identified the emergence of new threats and capabilities which have the potential to affect NORAD’s ability to deter, detect, and defeat threats to Canada and the U.S. The recommendations presented address current and emerging threats, ensuring our ability to monitor, control, and if necessary respond.”²² Specifically addressing cyberspace, the NORAD Strategic Review stated:

NORAD must be aware of current and emerging cyberspace threats and the means by which NORAD’s systems will be protected in order to meet their mission requirements. Therefore, NORAD must develop agreements and processes with trusted organizations and agencies to better analyze, characterize, assess, and share the impact of cyberspace events on NORAD operations, and the steps taken to defend NORAD networks against cyberspace-attacks.²³

Improvement of information sharing processes with cyberspace organizations and examination of new relationships can fill operational gaps to enhance NORAD mission assurance. (Canada’s Department of National Defence) and (U.S.’ Department of Defense) *should examine NORAD’s potential roles and responsibilities in providing binational Cyberspace Warning for North America.* (Emphasis added.)²⁴

²¹ Marcus Weisgerber, “Interview: General Charles Jacoby,” *Defense News*, 19 Jul 2014, <http://www.defensenews.com/article/20140719/DEFREG02/307190018/Interview-Gen-Charles-Jacoby>.

²² NORAD Strategic Review (Final Report), 18 Nov 2014, cover memorandum.

²³ Ibid., 22.

²⁴ Ibid., 23.

E. CYBER WARFARE COMPONENTS

1. Current Cyberspace Threat Actors

In his testimony to the Senate Select Committee on Intelligence on January 29, 2014, James Clapper (Director of National Intelligence) provided an overview of the various international cyber threat actors currently challenging the U.S.:

We assess that computer network *exploitation* and *disruption* activities such as denial-of-service attacks will continue. Further, we assess that the likelihood of a *destructive* attack that deletes information or renders systems inoperable will increase as malware and attack tradecraft proliferate.²⁵

First, Director Clapper highlighted his growing concerns regarding the evolving Russian cyber threat:

Russia presents a range of challenges to U.S. cyber policy and network security. Russia seeks changes to the international system for Internet governance that would compromise U.S. interests and values. Its Ministry of Defense (MOD) is establishing its own cyber command, according to senior MOD officials, which will seek to perform many of the functions similar to those of the U.S. Cyber Command.²⁶

As an example, the FireEye network security company stated they had reason to believe an “advanced persistent threat” (APT) from Russia had been operating since at least 2007, and was engaged in espionage against political and military targets. The report outlined how it was believed Russian hackers had targeted the Georgian Ministry of Defense; interfered with the Bulgarian, Polish and Hungarian governments; targeted Baltic military forces supporting U.S. Army training; and targeted several North Atlantic Treaty Organization (NATO) organizations.²⁷

²⁵ U.S. Senate, Select Committee on Intelligence, “Worldwide Threat Assessment of the U.S. Intelligence Community, 24 Jan 2014,” accessed on 20 Apr 2015, <http://www.intelligence.senate.gov/140129/clapper.pdf>.

²⁶ “Russia Preparing New Cyber Warfare Branch, Military Officials Say,” *Softpedia*, accessed 17 Dec 2014, <http://news.softpedia.com/news/Russia-Preparing-New-Cyber-Warfare-Branch-Military-Official-Says-376807.shtml>.

²⁷ Pierluigi Paganini, “APT28: Fireeye Uncovered a Russian Cyber Espionage Campaign,” *Security Affairs*, 29 Oct 2014, accessed 17 Dec 2014, <http://securityaffairs.co/wordpress/29683/intelligence/apt28-fireeye-russian-espionage.html>.

Director Clapper then identified to the Select Committee how China was also becoming a serious cyberspace threat to the Nation:

China's cyber operations reflect its leadership's priorities of economic growth, domestic political stability, and military preparedness... Internationally, China also seeks to revise the multi-stakeholder model of Internet governance while continuing its expansive worldwide program of network exploitation and intellectual property theft.²⁸

Underscoring this threat, in May of 2014, the U.S. Department of Justice indicted five members of the Chinese People's Liberation Army (PLA), charging these individuals with hacking into computer networks owned by the U.S. Steel Corporation, Westinghouse Electric, and other major corporations. The Justice Department indictment specifically focused on "Unit 61398," acknowledged as being the Shanghai-based cyber unit of the PLA. While acknowledging countries conduct espionage for national security purposes, the indictment charged it was illegal for China to employ national intelligence assets to steal U.S. corporate secrets in order to gain an economic advantage.²⁹

Director Clapper also warned the Committee about two other serious cyber threat actors. "Iran and North Korea are unpredictable actors in the international arena. Their development of cyber espionage or attack capabilities might be used in an attempt to either provoke or destabilize the U.S. or its partners."³⁰

Regarding Iran, U.S. Representative Peter Hoekstra (R-Michigan) stated, "Iran has boosted its cyber capabilities in a surprisingly short amount of time and possesses the ability to launch successful cyber attacks on American financial markets and its infrastructure."³¹

²⁸ U.S. Senate, Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community, 24 Jan 2014."

²⁹ Michael Schmidt and David Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *New York Times*, 19 May 2014, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberespionage.html?_r=0.

³⁰ U.S. Senate, Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community, 24 Jan 2014."

³¹ U.S. House Committee on Foreign Affairs, Joint Subcommittee Hearing, "Iran's Support for Terrorism Worldwide," 4 Mar 2014, accessed on 4 Apr 2015, <http://docs.house.gov/meetings/FA/FA13/20140304/101832/HHRG-113-FA13-20140304-SD001.pdf>.

Finally, North Korea has expended enormous resources to develop its cyber warfare cell called “Bureau 121” under the General Bureau of Reconnaissance, a spy agency run by the North Korean military.³² South Korean intelligence contends Bureau 121 has repeatedly conducted cyber attacks against numerous South Korea businesses, to include incidents in 2010 and 2012 targeting banks and media organizations. Pyongyang rejects these charges.³³

Thus, we clearly see the Intelligence Community’s rising concern about the cyberspace threat posed by several potentially hostile nations, and the general consensus that these global threats are indeed serious and not abating.

2. Typical Cyber Weapons

In their article “Cyber-Weapons,” Thomas Rid and Peter McBurney state there is no internationally agreed-upon definition of a cyber weapon. Therefore, they proposed the following definition: “A cyber weapon is seen as a subset of weapons, more generally as computer code that is used, or designed to be used, with the aim of threatening or causing *physical, functional, or mental harm* to structures, systems, or living beings.” (Emphasis added.)³⁴

Expanding upon this proposed definition, in his book *Cyberattack*, Paul Day proposed four levels of cyber weapons:³⁵

- Level 1. “Dual use” software tools provided with a computer’s organic operating system, such as network monitoring tools, which can be converted into hacking tools and exploit security vulnerabilities.

³² Ju-Min Park and James Pearson, “In North Korea, Hackers Are a Handpicked, Pampered Elite,” *Reuters*, 5 Dec 2014, <http://www.reuters.com/article/2014/12/05/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205>.

³³ Kyung Lah and Greg Botelho, “Watch Out World: North Korea Deep Into Cyber Warfare, Defector Says,” *Cable News Network*, 18 Dec 2014, <http://www.cnn.com/2014/12/18/world/asia/north-korea-hacker-network/index.html>.

³⁴ Thomas Rid and Peter McBurney”Cyber-Weapons,” *The Rusi Journal*, Feb/Mar 2012, 6–13, accessed 21 Apr 2015, https://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf.

³⁵ Paul Day, *Cyberattack* (London, UK: Carlton Publishing Group, 2013), 120–122.

- Level 2. Software tools that can be downloaded for computer security purposes that are then abused to compromise networks and computers. This software is specifically designed to allow skilled operators to test and penetrate system security, but in the wrong hands can subvert a network.
- Level 3. Malware designed only to exploit and infect other computers. Examples include RAT, spyware, and botnet clients. Again, these programs are widely available on the Internet.
- Level 4. Purposely built cyber weapons covertly developed by nation states with the expressed intention of waging cyber warfare. The most famous example is the “Stuxnet” worm discovered in 2010. (This level would match cyber weapon attacks as outlined by Rid and McBurney.)

3. Concept of “Cyber Attack”

In order to discuss the merits of any proposed cyber attack warning policy, it would be helpful to have a clear definition of what specifically defines a “cyber attack.”

Media Definitions. While the news media repeatedly warns us about “cyber attacks,”³⁶ there currently are no uniformly agreed-upon terms to describe cybersecurity activities. Typical cyber actions are often publically described as:³⁷

- “Cyber-vandalism” or “hacktivism” (defacing or otherwise temporarily interfering with public access websites.)
- “Cyber-crime” or “cyber-theft” (defrauding individuals to obtain their personal identification data, or actual theft of funds from financial accounts.)
- “Cyber-espionage” (covertly stealing sensitive or proprietary information.)
- “Cyber-warfare” (conducting military operations using cyber means.)

³⁶ “Cyber Attacks on South Korean Nuclear Power Operator Continue,” *The Guardian*, 28 Dec 2014, accessed 21 Apr 2015, <http://www.theguardian.com/world/2014/dec/28/cyber-attacks-south-korean-nuclear-power-operator>.

³⁷ “At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues,” *National Academy of Science*, 2014, vii, accessed 17 Dec 2014, http://www.nap.edu/openbook.php?record_id=18749.

Popular cyber terms used in the media include “breach,” “compromise,” “intrusion,” “exploit,” “hack,” “incident,” and “attack.”³⁸ So what is the difference between these various terms? Specifically, from a military viewpoint, what should be meant by a “cyber attack”?

NATO Definition. We begin by defining an “act of aggression” as being “the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations.”³⁹ Examples of acts of aggression outlined by the United Nations in its resolution include:

- The invasion or attack by the armed forces of a State into the territory of another State.
- Bombardment by the armed forces of a State against the territory of another State, or the use of any weapons by a State against the territory of another state.
- The blockade of the ports or coasts of a State.
- An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State.⁴⁰

Given this general definition of an act of aggression, what does it mean to conduct a “cyber attack?”

To answer this issue, beginning in 2009, NATO undertook a three-year project to identify the international laws applicable to cyber warfare, with a goal of defining specific rules governing such conflicts.

Working with twenty international law scholars and cyber practitioners, this working group eventually published their *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013.

³⁸ Ibid., 30.

³⁹ United Nations General Assembly Resolution 3314 (XXIX), “Definition of Aggression,” Article 1 (Dec 14, 1974), accessed 18 May 2014, <http://www.un-documents.net/a29r3314.htm>.

⁴⁰ Ibid., Article 3.

First, the Tallinn group developed a general definition of the “use of force” for cyber operations: “A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”⁴¹

The group found focusing on the “scale and effects” of a cyber operation was a useful approach when attempting to distinguish between cyber acts which unmistakably qualify as use of force (e.g., such as acts that injure people or damage property) from cyber acts which do not cause physical harm. Used this way, “scale and effects” effectively captures the qualitative factors to be considered in evaluating whether a cyber operation reached the level of other kinetic actions analogous to a use of force.⁴²

The group next developed a set of eight specific factors to consider in judging whether a specific cyber operation actually constituted the “use of force.” As stated in the *Tallinn Manual*, these include:

- Severity. Consequences involving physical harm to individuals or property will in and of themselves qualify the act as a use of force...the scope, duration, and intensity of the event will have great bearing on the appraisal of their severity.
- Immediacy. The sooner consequences manifest, the less opportunity States have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects.
- Directness. Cyber operations in which the cause and effect are clearly linked are more likely to be characterized as uses of force.
- Invasiveness. As a rule, the more secure a targeted cyber system, the greater the concern as to its penetration. For example, cyber operations targeting State domain names (e.g., “.mil” or “.gov”) could be considered more invasive than cyber operations directed at non-State domain names (e.g., “.com” or “.net.”)

⁴¹ Michael N. Schmitt, edit., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge, UK: University Press, 2013.) (Note: Tallinn is the capital of Estonia, where the first modern cyber attack occurred, where the NATO Cooperative Cyber Defense Center of Excellence is now located, and where this manual was eventually developed.)

⁴² Ibid., 48.

- Measurability of Effects. The more quantifiable and identifiable a set of consequences, the easier it will be for a State to assess the situation when determining whether the cyber operation in question has reached the level of a use of force.
- Military Character. The closer the connection between the cyber operation and military operations, the more likely it will be deemed a use of force.
- State Involvement. The clearer and closer a nexus between a State and cyber operations, the more likely it is that other States will characterize them as uses of force by that State.
- Presumptive Legality. Finally, the group clarified that acts not forbidden by international law are permitted and are presumptively legal. Thus, propaganda, psychological operations, espionage, economic pressure, etc., are all actions allowed by international law. Thus, cyber operations falling into these internationally legal categories will be less likely to be considered by States as uses of force.⁴³

Using these specific factors, the Tallinn group then developed a definition of the “threat of force” under cyber operations: “A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force.”⁴⁴

Finally, linking all previous definitions into a coherent concept, the Tallinn group developed a definitive definition of what constitutes a genuine “cyber attack”:

A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.⁴⁵

Thus, after considerable legal deliberations and debate, the Tallinn group developed a definition of “cyber attack” useful in policy development, military strategies, and international affairs. It excludes non-lethal activities (such as cyber-crime and cyber-espionage) and allows for both state and non-state actors.

⁴³ Ibid., 48–51.

⁴⁴ Ibid., 52.

⁴⁵ Ibid., 106.

More importantly, the NATO definition clearly provides a logical connection between the legal concepts of “an act of aggression,” “use of force,” “threat of force,” “armed attack,” and “self-defense.” And it provides useful factors for consideration in determining whether the “scale and effects” of a specific cyber operation constitutes an actual armed attack upon a State.

Expressing similar concerns about growing worldwide cyberspace threats, NATO endorsed a new “Enhance Cyber Defence Policy” during its 2014 North Atlantic Council Summit. In its published Declaration, NATO stated:

The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks...Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance.⁴⁶

Former NATO Commander Definition. Interestingly, in January 2015, Admiral James Stavridis (NATO Commander from 2009–2013) disagreed with this specific NATO definition. He stated the *Tallinn Manual* definition of cyber attack was “far too simplistic to account for the nuances of cyberwarfare. It sets a dangerously high threshold for a domain with comparatively low barriers to entry.”⁴⁷

Stavridis proposed there are three elements to “cyberforce”: Intelligence (understanding the target environment), cyberweapons (the actual computer code, usually target-specific with a short shelf life), and intent (a calculated human decision). He then proposes it is specifically the cyberweapon which defines whether cyberforce approaches the level of a genuine armed attack.⁴⁸

⁴⁶ NATO Wales Summit Declaration, 5 Sep 2014, paras 72–73, accessed 17 Dec 2014, <http://www.cfr.org/nato/wales-summit-declaration/p33394>.

⁴⁷ Adm James Stavridis, “Incoming: What is a Cyber Attack?,” *Signals*, 1 Jan 2015, accessed 21 Apr 2015, <http://www.afcea.org/content/?q=node/13832>.

⁴⁸ Ibid.

For example, Stavridis outlines the 2012 “Shamoon” virus that infected Saudi Aramco, the world’s largest State-owned oil company. This cyber operation erased data from computer memories which the company could not reconstitute. Also, company systems were down for two weeks, resulting in adverse global economic affects. Finally, more than 30,000 workstations were replaced to rid the corporation network of malware. This action “is a far better measure of cyberforce than simply concentrated personal injury or physical damage. Yet, according to the *Tallinn Manual*, Shamoon was not a cyber attack.”⁴⁹

Therefore, Stavridis offers his own alternative definition:

A cyber attack is the deliberate projection of cyberforce resulting in kinetic or nonkinetic consequences that threaten or otherwise destabilize national security, harm economic interests, create political or cultural instability; or hurt individuals, devices or systems.⁵⁰

This may become a more useful definition for future military planners, as it broadens threats from cyberspace operations to include those actions which inflict economic harm or national security instability.

4. Military Cyberspace Definitions

Finally, from a Department of Defense (DOD) perspective, military cyberspace missions can be characterized using the following unclassified definitions:

Department of Defense Information Networks (DODIN). “The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.”⁵¹

⁴⁹ Ibid.

⁵⁰ Ibid.

⁵¹ Department of the Army, Field Manual 3-38, “Cyber Electromagnetic Activities,” 3-7 Feb 2014, accessed 21 Apr 2015, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf.

DODIN Operations. “Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks.”⁵² DODIN operations are the traditional methods we all think of to preserve data availability, integrity, confidentiality, and user authentication. These operations include configuration control and system patches, user training, physical security, firewalls, and data encryption. Many DODIN activities are conducted through regularly scheduled events and updates.

Defensive Cyberspace Operations (DCO). These are operations which respond to unauthorized activity or alert/threat information against the DODIN. DCO can be both “passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.”⁵³ DCO consists of both internal defensive measures and DCO Response Actions (DCO-RA):

“Internal defense measures” are conducted within the DODIN. These are defined as being “defensive tools and techniques [which] are designed to find, fix and finish anomalous network activity using rule, signature and behavioral-based techniques.”⁵⁴

“DCO-RA” are defensive measures taken outside the defended network to protect DOD cyberspace capabilities. Once sources of a cyber attack are identified, response actions (such as custom-made computer code) may be implemented to defend friendly cyberspace systems.⁵⁵

Offensive Cyberspace Operations (OCO). These are “operations intended to project power by the application of force in and through cyberspace.”⁵⁶ OCO focuses effects in cyberspace to influence or degrade enemy weapon systems, command and control processes, critical infrastructures, etc.

⁵² Ibid., 3–7.

⁵³ Ibid., 3–6.

⁵⁴ Ibid., 3–6.

⁵⁵ Ibid., 3–6.

⁵⁶ Ibid., 3–2.

Cyberspace Attack. Cyberspace activities that create denial effects (by degrading, disrupting or destroying access to, operation of, or availability of a target) or that manipulate (by controlling or changing an adversary's information or networks.)⁵⁷

All of these overlapping relationships are illustrated in Figure 9.

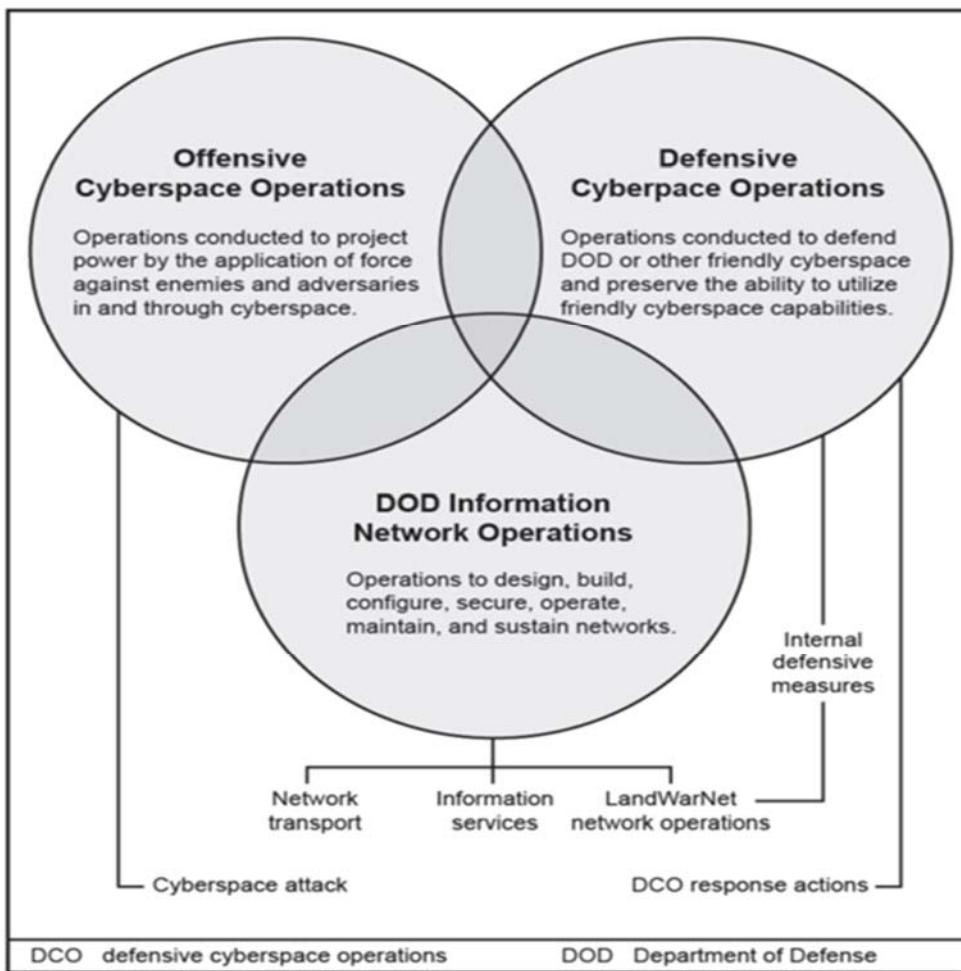


Figure 9. DOD Cyberspace Operations.⁵⁸

⁵⁷ Ibid., 3-3.

⁵⁸ Ibid., 3-2.

As can be seen, the topic of “cyber attack” involves not only various potential definitions of what a cyber attack actually entails, but also what means are available to either defensively or offensively respond to such an attack. While these definitions remain fluid, they provide an essential conceptual foundation to allow policy makers to consider how “cyber attack warning” might specifically be implemented by NORAD.

F. KEY U.S. MILITARY CYBER ORGANIZATIONS

1. Department of Defense

The Department of Defense (DOD) is the executive department of the U.S. charged with coordinating all agencies and functions concerned directly with the U.S. Armed Forces. (See Figures 10 and 11.)

Headed by the Secretary of Defense (SecDef), DOD has three subordinate military departments: the Departments of the Army, the Navy, and the Air Force. DOD’s theater military operations are managed by nine Combatant Commands. (Note: NORAD is not part of DOD, as it is a separate, binational command reporting to both the U.S. and Canada.)

2. Joint Chief of Staff

Within the civilian DOD falls the military Joint Chiefs of Staff (JCS), which consists of the Chairman JCS (CJCS); the Vice Chairman; the Chiefs of Staff of the Army, Navy, and Air Force; the Commandant of the Marine Corps; the Chief of the National Guard Bureau, and the administrative Joint Staff (JS). (See Figure 11.)

The CJCS serves as the primary military adviser to the president, to the SecDef, and to the National Security Council. The JCS have no executive authority to command combat forces, which are assigned directly to Combatant Commands.⁵⁹

⁵⁹ U.S. Department of Defense, “About the Joint Chiefs of Staff,” accessed 30 Dec 2014, <http://www.jcs.mil/About.aspx>.

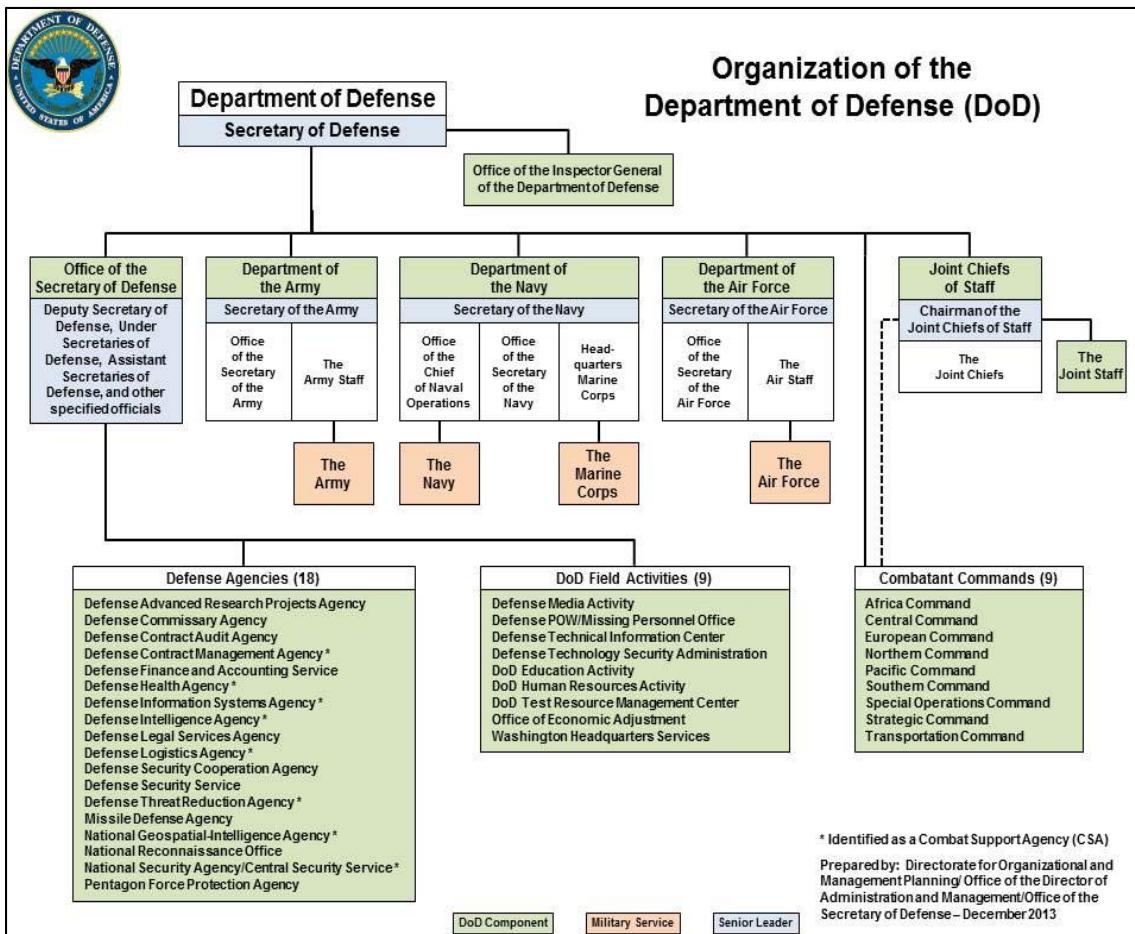


Figure 10. DOD Organizational Chart.⁶⁰



Figure 11. DOD and JCS Emblems.

⁶⁰ U.S. Department of Defense, “Organization of the Department of Defense,” accessed 30 Dec 2014, <http://odam.defense.gov/OMP/Functions/OrganizationalPortfolios/OrganizationandFunctionsGuidebook.aspx>.

3. U.S. Northern Command

Created in 2002, USNORTHCOM is the Combatant Command charged with conducting homeland defense, civil support and security cooperation to defend and secure the U.S. and its interests within the North America. (See Figure 12.)

“USNORTHCOM’s area of responsibility includes air, land and sea approaches and encompasses the continental U.S., Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico, the Straits of Florida, and portions of the Caribbean region to include The Bahamas, Puerto Rico, and the U.S. Virgin Islands. The commander of USNORTHCOM is responsible for theater security cooperation with Canada, Mexico, and The Bahamas.”⁶¹

“USNORTHCOM consolidates under a single unified command existing missions that were previously executed by other DOD organizations. This consolidation provides better unity of command, which is critical to mission accomplishment.”⁶²

USNORTHCOM is located at Peterson AFB, Colorado.



Figure 12. USNORTHCOM Emblem.

⁶¹ U.S. Northern Command, “About USNORTHCOM,” accessed 30 Dec 2014, <http://www.northcom.mil/AboutUSNORTHCOM.aspx>

⁶² Ibid.

4. U.S. Strategic Command

“USSTRATCOM combines the synergy of the U.S. legacy nuclear command and control mission with responsibility for space operations; global strike; global missile defense; and global command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); and combating weapons of mass destruction.”⁶³ (See Figure 13.)

Per its mission statement, “USSTRATCOM conducts global operations in coordination with other Combatant Commands, Services, and appropriate U.S. Government agencies to deter and detect strategic attacks against the U.S. and its allies, and is prepared to defend the nation as directed.”⁶⁴

To execute its specific military cyberspace responsibilities, USSTRATCOM commands the subordinate U.S. Cyber Command (USCYBERCOM).⁶⁵

USSTRATCOM is located at Offutt AFB, Nebraska.



Figure 13. USSTRATCOM Emblem.

⁶³ U.S. Strategic Command, “Mission and Priorities,” accessed 12 Feb 2014, <https://www.stratcom.mil/about/>.

⁶⁴ U.S. Strategic Command, “Mission and Priorities,” accessed 12 Feb 2014, <https://www.stratcom.mil/mission/>.

⁶⁵ U.S. Strategic Command, “Mission and Priorities,” accessed 12 Feb 2014, https://www.stratcom.mil/functional_components/.

5. U.S. Cyber Command

Created in 2009, USCYBERCOM “unifies the direction of cyberspace operations, strengthens DOD cyberspace capabilities, and integrates and bolsters DOD’s cyber expertise.” (See Figure 14.)

“USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to:

- Direct the operations and defense of specified Department of Defense information networks and;
- Prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.”

USCYBERCOM is located in Fort Meade, Maryland, and is co-located with the National Security Agency (NSA). The Commander, USCYBERCOM, also serves as the Director, NSA.



Figure 14. USCYBERCOM Emblem.

G. KEY CANADIAN MILITARY CYBER ORGANIZATIONS

1. Department of National Defence

The Department of the National Defence (DND) is the executive department of the Canadian government charged with coordinating all agencies and functions concerned directly with national security and the Canadian Armed Forces. (See Figures 15 and 16.)

Headed by the Minister of National Defence (MND), DND has three subordinate military departments: the Canadian Army, the Royal Canadian Navy, and the Royal Canadian Air Force. (Note: Again, NORAD is also not part of DND, as it is a separate, binational command reporting to both the U.S. and Canada.)

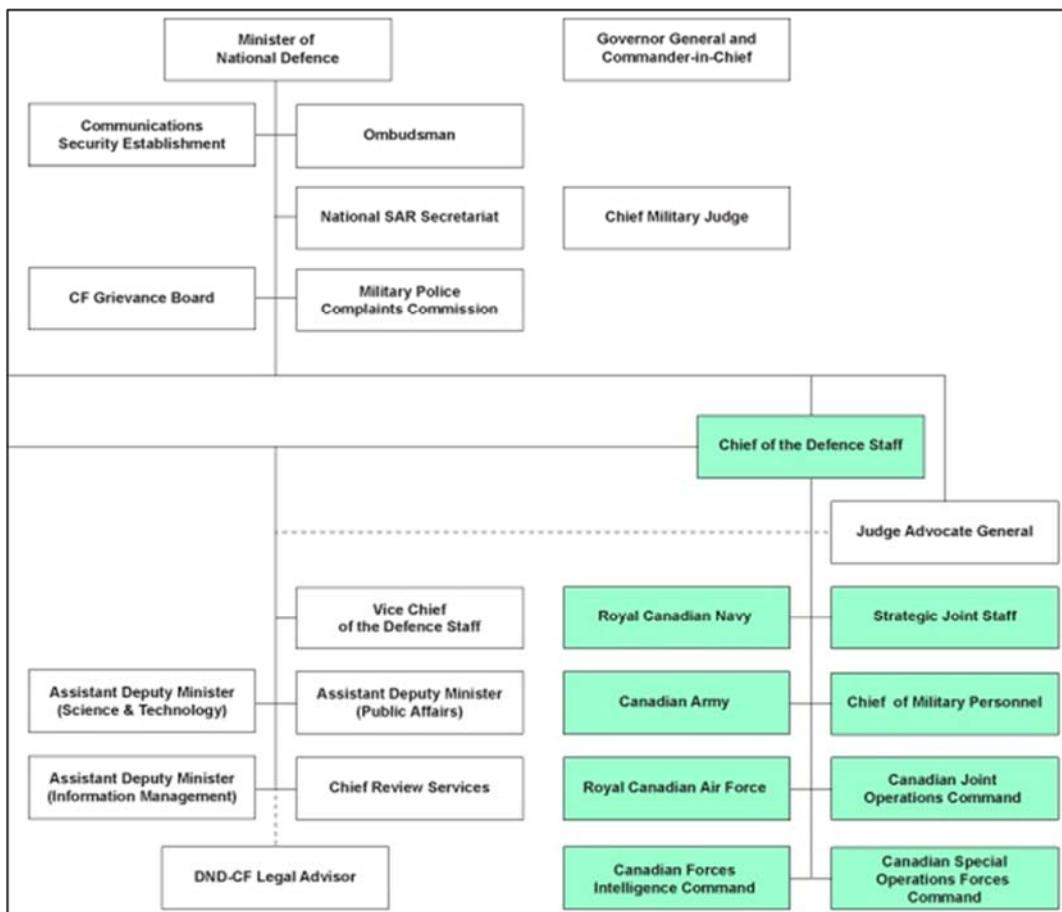


Figure 15. DND Organizational Chart.⁶⁶

⁶⁶ Canadian Department of National Defence, “Organizational Structure,” accessed 2 Jan 2015, <http://www.forces.gc.ca/en/about-org-structure/index.page>.



Figure 16. DND and SJS Crests.

2. Strategic Joint Staff

Within the civilian DND falls the Chief of the Defence Staff (CDS), the Commanders of the Canadian Army, Royal Canadian Navy, and Royal Canadian Air Force; and the administrative Strategic Joint Staff (SJS). (See Figure 16.)

The CDS serves as the principal military adviser to the prime minister, the MND, and the Government of Canada.⁶⁷ The SJS have no executive authority to command combat forces, which are directly assigned under the Commander, CJOC.

⁶⁷ Canadian Department of National Defence, “Chief of the Defence Staff,” accessed 2 Jan 2015, <http://www.forces.gc.ca/en/about-org-structure/chief-of-defence-staff.page>.

3. Canadian Joint Operations Command

Established in 2012 in Ottawa, Ontario, “CJOC is responsible for conducting full-spectrum Canadian Armed Forces operations at home, on the continent of North America, and around the world.”⁶⁸ (See Figure 17.)



Figure 17. CJOC Crest.

Integrating the operations of three previously separate military commands, “CJOC directs Canadian military operations from their earliest planning stages through to mission closeout, and ensures that national strategic goals are achieved.”⁶⁹

CJOC coordinates all military operations via its Canadian Forces Integrated Command Centre (CFICC). The only military operations CJOC does not command are those missions carried out by:

- Canadian Special Operations Forces Command.
- North American Aerospace Defense Command.⁷⁰

⁶⁸ Canadian Department of National Defence, “Canadian Joint Operations Command,” accessed 2 Jan 2014, <http://www.forces.gc.ca/en/about-org-structure/canadian-joint-operations-command.page>.

⁶⁹ Ibid.

⁷⁰ Ibid.

4. Canadian Forces Information Operations Group

Falling under the DND Assistant Deputy Minister for Information Management, the Director General of Information Management Operations (DGIMO) is responsible for overseeing CFIOG, which is charged with conducting Electronic Warfare (EW), Signals Intelligence (SIGINT), and Network Defense in support of Canadian Forces operations. (See Figure 18.) (Note: DGIMO is dual-hatted as the CJOC Cyber Component Commander.)

CFIOG operates the Canadian Forces Electronic Warfare Centre (CFEWC), the Canadian Forces Network Operation Centre (CFNOC), and Canadian Forces Station (CFS) Leitrim itself, Canada's oldest signal intelligence station.⁷¹

Overall, DGIMO and CFIOG together can be considered equivalent to U.S. Cyber Command, while CFNOC corresponds to more tactical, military service-operated cyber organization such as the U.S. Army Cyber Command, the U.S. Fleet Cyber Command or 24th Air Force.



Figure 18. DGIMO, CFIOG and CFNOC Crests.

⁷¹ Jerry Proc, ‘Radio Communications and Signals Intelligence in the Royal Canadian Navy, CFS Leitrim’ accessed 21 Apr 2015, <http://jproc.ca/rrp/leitrim.html>.

H. MILITARY CYBER EVENT CONFERENCES

1. Cyber Event Conferences

The CJCS has established emergency conferencing procedures to allow military commands around the world to simultaneously connect and discuss urgent military events. One type of cyberspace event consultation was previously entitled “Operation Gladiator Phoenix” conferences:⁷²

(U) Operation GLADIATOR PHOENIX Conference (OGPC). The OGPC allows USCYBERCOM to rapidly investigate any significant cyber activities and determine if there is a possible cyber attack on the U.S., its national security, civilian or military personnel, critical infrastructure, and/or other national assets or interests.⁷³

Managed by USCYBERCOM, these classified, encrypted conferences are used by cyberspace technical experts to discuss real-time network concerns. Recently, OGP conferences were split into two new discussion groups and renamed:

- “Cyber Watch Conferences” now provide a specialized forum for operational watch centers to identify and troubleshoot anomalous cyberspace indications, conduct checks to verify circuits are serviceable, communication encryption devices are functioning, satellite relay systems are operative, etc.
- “Cyber Event Conferences” now allow senior decision-makers to discuss potential operational impacts with each other, and to deliberate what follow-on cyberspace actions might be required.

Typically, whenever USCYBERCOM detects a cyberspace event, it notifies all applicable command centers (such as Headquarters NORAD and USNORTHCOM) using either a “Cyber Watch Conference” or “Cyber Event Conference” (depending on the severity of the cyber event) to resolve any resulting issues. (See Figure 19.)

⁷² U.S. Department of Defense, “Emergency Action Procedures of the Chairman of the Joint Chiefs of Staff, Volume VI, Emergency Conferences (U),” 14 Sep 2012. (Note: Information presented are from unclassified paragraphs.)

⁷³ Ibid., II-15.

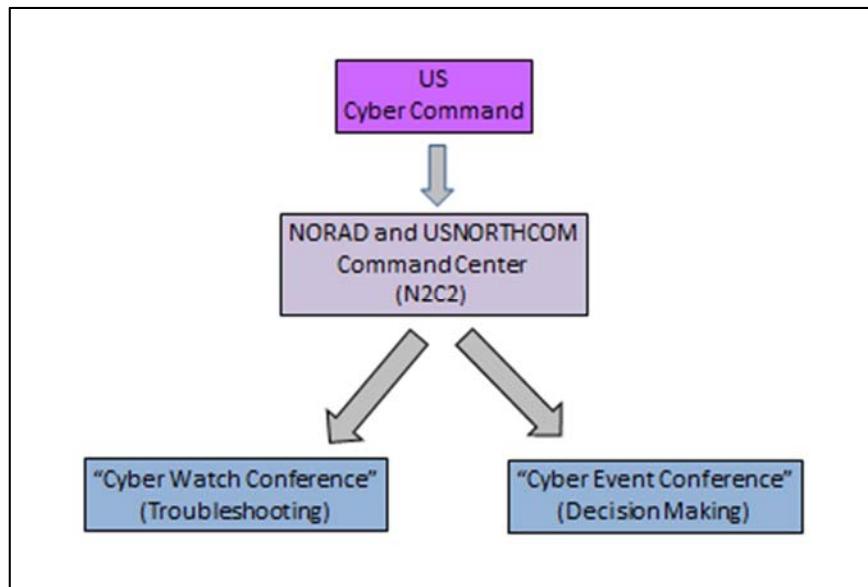


Figure 19. Cyber Event Conferences.

2. National Event Conference

Another, more senior conference (managed by the Pentagon) is entitled the “National Event Conference” or NEC, in which agencies are brought together for situational awareness regarding a significant national event.

One significant situation that can trigger a NEC is a “cyberspace event,” defined as “...any significant loss or serious threat of loss of networks or data (e.g., critical cyberspace links or nodes, cyberspace mission data providing assets) that threaten U.S. national security or interests.”⁷⁴

During a cyber NEC, Commander USCYBERCOM is required to make an official “Cyberspace Attack Assessment” to U.S. (but not currently Canadian) national leadership using formally-defined assessment criteria.⁷⁵ (See Table 1.)

⁷⁴ Ibid., II-14.

⁷⁵ Ibid., II-14.

UNCLASSIFIED	
YES	In the judgment of CDRUSCYBERCOM, a verified Cyberspace Attack has occurred, is occurring or is imminent.
CONCERN	In the judgment of CDRUSCYBERCOM, a Cyberspace Attack may be in progress or is imminent. The situation is still under assessment and may warrant implementation of appropriate measures and/or plans to enhance cyberspace responsiveness and inter-agency awareness.
NO	In the judgment of CDRUSCYBERCOM, a verified Cyberspace Attack has not occurred, nor is one in progress.
PENDING	The judgment of CDRUSCYBERCOM will be provided as soon as possible. No assessment is available at this time. There is inadequate information available to assess whether a Cyberspace Attack is or may be occurring or is imminent.
UNCLASSIFIED	

Table 1. Cyberspace Attack Assessment Criteria.⁷⁶

⁷⁶ Ibid., II-14.

Finally, the NORAD and USNORTHCOM Command Center (N2C2) acts as the central point of contact and coordinator for participation in all national conferences for both Commands. (See Figure 20.)



Figure 20. NORAD-USNORTHCOM Command Center.⁷⁷

This joint command center integrates missile warning, air warning, maritime warning, land operations, and cyberspace operations, bringing the Commands' multiple missions together to create greater synergy.

However, due to U.S. information classification restrictions, Canadian personnel must exit any national event conference once specific "US-only" classified topics are being discussed.

⁷⁷ Lockheed Martin, "Integrated Space Command & Control (ISC2)," accessed 13 Jan 2015, <http://www.lockheedmartin.com/us/products/isc2.html>.

I. SUMMARY

Since 1958, NORAD has a proven history of adapting and evolving to meet changing military defense challenges using new technology—from its early years providing ground-based radar warning of approaching Soviet bombers, to ground-based radar warning of in-bound Soviet ICBMs, to satellite-based warning of any missile launch occurring around the world, to extended radar warning of approaching cruise missiles, to the warning of suspect maritime vessels approaching North America.

NORAD has sole responsibility for receiving early warnings from numerous space-based and ground-based sensors and developing an integrated North American attack assessment. And because all of the sensors feeding into NORAD travel across the broader “information superhighway,” there exists a genuine risk of potentially hostile nations conducting damaging cyberspace operations against NORAD (to include blinding NORAD to actual threats or feeding the Command false information for incorrect action.) With the recent increase in world-wide cyberspace events, NORAD has thus begun examining its own potential role in this new operational domain.

As we have seen, an exact definition defining the meaning of “cyber attack” remains in flux. Despite this lack of definition, both the U.S. and Canada have been quick to establish new, dedicated military organizations specializing in cyberspace operations. Further, military cyberspace event conferences now share warning information between U.S. Combatant Commands around the world, to include the NORAD-USNORTHCOM Command Center. (One area of concern: current U.S. policies restrict the sharing of certain classified information with Canadian NORAD members.)

Given this historical, terminology, organizational and event conference background, we can now review the principle U.S. and Canadian strategic documents which establish cyberspace policies for both countries.

III. LITERATURE REVIEW

A. INTRODUCTION

Cyberspace warning is influenced by a host of international, governmental and military policies and guidance. Both the U.S. and Canada governments have published many documents providing guidance to military commands at the strategic, operational, and tactical levels. A brief survey of key directives helps clarify the roles and authorities of each level of government in dealing with potential cyberspace attacks.

B. NORAD GUIDANCE

1. NORAD Agreement

On May 12, 1958, the “NORAD Agreement” statutorily establishing the “North American Air Defense Command” (NORAD) was formalized between the U.S. and Canadian governments. The Agreement has then reviewed, revised, and renewed approximately every five years (most recently, on 28 April 2006).⁷⁸

During the March 1996 renewal, NORAD’s missions were redefined to be “aerospace warning” and “aerospace control” for North America.⁷⁹

Then, during the May 2006 renewal, the new “maritime warning” mission was added to the command’s existing aerospace warning and control missions. In this renewal, the two nations outlined their mutual understanding of the current political, military and threat environment in the Agreement’s preamble:

MINDFUL that in the years since the first NORAD Agreement was concluded on May 12, 1958, NORAD, as a distinct command, has evolved to address the continuing changes in the nature of the threats to North America *and that it will need to continue to adapt to future shared security interests* (emphasis added);

⁷⁸ North American Aerospace Defense Command, “NORAD Agreement,” accessed 3 Feb 2014, <http://www.norad.mil/AboutNORAD/NORADAgreement.aspx>.

⁷⁹ Ibid.

AWARE of dramatic changes in the geostrategic environment and in the threats to North America, as illustrated by the terrorist attacks of September 11, 2001, in terms of the nations, non-state actors or terrorist groups that might choose to challenge North American security, the symmetry and asymmetry of the weapons and methods they could employ, and the transnational and global nature of these threats;

ACKNOWLEDGING that space has become an important dimension of national interest and has become an increasingly significant component of most traditional military activities, and that a growing number of nations have acquired or have ready access to space services that could be used for strategic and tactical purposes against the interests of the U.S. and Canada;

REALIZING that a shared understanding and awareness of the activities conducted in their respective maritime approaches, maritime areas and inland waterways, including the capacity to identify vessels of potential interest, are critical to their ability to monitor, control, and respond to threats so that their shared security is ensured;

DESIRING to ensure that their respective and mutual defense requirements are met in the current and projected geostrategic circumstances; HAVE AGREED as follows...⁸⁰

Four Articles of the Agreement then outline the specific areas of mutual agreement. Under Article I, “NORAD Missions,” specific definitions were provided outlining the binational Command’s now-three core missions:

Aerospace warning consists of processing, assessing and disseminating intelligence and information related to man-made objects in the aerospace domain and the detection, validation, and warning of attack against North America whether by aircraft, missiles or space vehicles, utilizing mutual support arrangements with other commands and agencies.

Aerospace control consists of providing surveillance and operational control of the airspace of the United States and Canada. “Operational control” is the authority to direct, coordinate and control the operational activities of forces assigned, attached or otherwise made available to NORAD.

⁸⁰ U.S. Department of State, “NORAD Agreement,” 28 Apr 2006, accessed 21 Apr 2015, <http://www.state.gov/documents/organization/69727.pdf>.

Maritime warning consists of processing, assessing and disseminating intelligence and information related to the respective maritime areas and internal waterways of, and the maritime approaches to, the U.S. and Canada, and warning of maritime threats to, or attacks against North America utilizing mutual support arrangements with other commands and agencies, to enable identification, validation, and response by national commands and agencies responsible for maritime defence and security.⁸¹

Thus, over the course of 50 years, NORAD has repeatedly reassessed, redefined, and updated its core operational missions based upon a constantly evolving threat. The NORAD Agreement clearly reflects the desire for NORAD to be able to adapt and defend against newly evolving military threats which each nation may jointly face.

2. NORAD Strategic Review

Completed by the NORAD headquarters staff in December 2014, the NORAD Strategic Review stated, “NORAD must be aware of current and emerging cyber threats and the means by with NORAD’s systems will be protected in order to meet their mission requirements. Therefore, NORAD must develop agreements and processes with mission partners to better analyze, characterize, assess, and *share the impact of cyber events on NORAD operations, and defend NORAD networks against cyber attacks. Currently, there is no formal U.S.-Canada process to collectively analyze, characterize and assess the operational impact of North American cyberspace events and the provide timely, simultaneous warning of attack/threat to the national leaderships of Canada and the U.S.*” (Emphasis added.)⁸²

“Improvement of information sharing processes with cyber mission partners and examination of new relationships can fill operational gaps to enhance NORAD mission assurance. *DND and DOD should examine NORAD’s potential roles and responsibilities in providing binational Cyberspace Warning for North America.*” (Emphasis added.)⁸³

⁸¹ Ibid.

⁸² North American Aerospace Defense Command, “NORAD Strategic Review (S//RELCAN),” 3 Dec 2014, 22. (Only unclassified paragraphs were quoted.)

⁸³ Ibid., 23.

C. U.S. NATIONAL CYBERSPACE GUIDANCE

1. Executive Branch

a. *National Strategy to Secure Cyberspace (2003)*

Recognizing the need to protect federal computers now connected via the “new” Internet, this Strategy directed the new Department of Homeland Security (DHS) become the “federal center of excellence for cyber-security.” The Strategy articulated five national priorities:

- I - A National Cyberspace Security Response System;
- II - A National Cyberspace Security Threat and Vulnerability Reduction Program;
- III - A National Cyberspace Security Awareness and Training Program;
- IV - Securing Governments’ Cyberspace; and
- V - National Security and *International Cyberspace Security Cooperation.*

(Emphasis added.)⁸⁴

Thus, a key feature of the National Cyber Strategy was the recommendation to work with international partners to develop international watch-and-warning networks in order to detect and prevent cyber attacks (a relevant information-sharing theme that will be repeated in numerous national guidance documents to follow.)

b. *Comprehensive National Cybersecurity Initiative (2008)*

A classified document, the CNCI outlined twelve reinforcing initiatives designed to help secure the Nation in cyberspace.⁸⁵ Initiative #10 is of particular interest:

⁸⁴ U.S. Department of Homeland Security, “National Strategy to Secure Cyberspace,” Feb 2003, accessed 10 Feb 2014, <http://www.dhs.gov/national-strategy-secure-cyberspace>.

⁸⁵ The White House, “Comprehensive National Cybersecurity Initiative,” Jan 2008, accessed 10 Feb 2014, <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>.

Initiative #10. Define and develop enduring deterrence strategies and programs. Our Nation’s senior policymakers must think through the long-range strategic options available to the United States in a world that depends on assuring the use of cyberspace. To date, the U.S. Government has been implementing traditional approaches to the cybersecurity problem—and these measures have not achieved the level of security needed. This Initiative is aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace *by improving warning capabilities, articulating roles for private sector and international partners*, and developing appropriate responses for both state and non-state actors. (Emphasis added.)⁸⁶

c. Cyberspace Policy Review (2009)

In an effort to establish his own administration’s guidance for cyberspace, President Obama directed a “clean slate” review assessing U.S. cybersecurity policies.⁸⁷ Cybersecurity policy includes:

Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, *international engagement*, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (Emphasis added.)⁸⁸

As a near-term accomplishment, the report specifically recommended the Nation should “develop U.S. Government positions *for an international cybersecurity policy framework and strengthen our international partnerships* to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.” (Emphasis added.)⁸⁹

⁸⁶ Ibid.

⁸⁷ U.S. Department of Homeland Security, “Cyberspace Policy Review,” 2009, iii, accessed 6 Feb 2014, <http://www.dhs.gov/publication/2009-cyberspace-policy-review>.

⁸⁸ Ibid., 2.

⁸⁹ Ibid., vi.

d. National Security Strategy (2010)

The National Security Strategy (NSS) is prepared by the executive branch to outline the key national security concerns of the United States, and how the current administration plans to specifically address those concerns. Under Part III, “Advancing our Interests,” the NSS states:

Strengthening Partnerships: Neither government nor the private sector nor individual citizens can meet this challenge alone—we will expand the ways we work together. *We will also strengthen our international partnerships* on a range of issues, including the development of norms for acceptable conduct in cyberspace; laws concerning cybercrime; data preservation, protection, and privacy; *and approaches for network defense and response to cyber attacks.* We will work with all the key players—including all levels of government and the private sector, nationally and internationally—to investigate cyber intrusion and to ensure an organized and unified response to future cyber incidents. Just as we do for natural disasters, we have to have plans and resources in place beforehand. (Emphasis added.)⁹⁰

e. U.S. International Strategy for Cyberspace (2011)

This document serves as the U.S.’ first, comprehensive International Strategy for Cyberspace. In Part III, “Policy Priorities,” the Strategy reviews Cyberspace policy priorities for economic growth, protecting national networks, enhancing law enforcement actions, promoting better Internet governance and freedoms, promoting international development, and military considerations. Regarding military initiatives, the Strategy outlines the following:

Build and enhance existing military alliances to confront potential threats in cyberspace. Cybersecurity cannot be achieved by any one nation alone, and greater levels of international cooperation are needed to confront those actors who would seek to disrupt or exploit our networks. This effort begins by acknowledging that the interconnected nature of networked systems of our closest allies, *such as those of NATO and its member states*, creates opportunities and new risks. Moving forward, the United States will continue to work with the militaries and civilian counterparts of our allies and partners *to expand situational awareness and shared warning systems, enhance our ability to work together in times*

⁹⁰ The White House, “National Security Strategy,” 2010, accessed 4 Feb 2014, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

of peace and crisis, and develop the means and method of collective self-defense in cyberspace. Such military alliances and partnerships will bolster our collective deterrence capabilities and strengthen our ability to defend the U.S. against state and non-state actors. (Emphasis added.)⁹¹

Overall, the International Strategy for Cyberspace establishes a roadmap allowing U.S. governments and agencies to better coordinate cyberspace policy with our partner nations. It also establishes an invitation to other nations to join in a common vision of innovation, interoperability, reliability and security.

Considering military efforts, “the United States will continue to work with the militaries and civilian counterparts of our allies and partners to expand situational awareness and shared warning systems, enhance our ability to work together in times of peace and crisis, and develop the means and method of collective self-defense in cyberspace.”⁹²

f. PPD-20, U.S. Cyber Operations Policy (2012)

This classified Presidential Policy Decision (PPD), described in an unclassified White House Fact Sheet, “establishes principles and processes for the use of cyberspace operations so that cyberspace tools are integrated with the full array of national security tools we have at our disposal. The policy provides a whole-of-government approach consistent with values we promote domestically and internationally as we have previously articulated in the International Strategy for Cyberspace.”⁹³ Later, in an open-press article, PPD-20 was described as being an 18-page “cyber policy roadmap” for the Pentagon that identifies the authority for the U.S. Cyber Command and the JCS to employ cyber weapons.⁹⁴

⁹¹ The White House, “Launching the U.S. International Strategy for Cyberspace,” 2011, accessed 11 Feb 2014, <http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace>.

⁹² *Ibid.*, 21.

⁹³ Federation of American Scientists, “Fact Sheet of Presidential Policy Directive 20,” accessed 14 Jan 2015, <http://fas.org/irp/offdocs/ppd/ppd-20-fs.pdf>.

⁹⁴ Mark Clayton, “Presidential Cyberwar Directive Gives Pentagon Long-Awaited Marching Orders,” *Christian Science Monitor*, 10 Jun 2013, accessed 14 Jan 2015, <http://www.csmonitor.com/USA/Military/2013/0610/Presidential-cyberwar-directive-gives-Pentagon-long-awaited-marching-orders-video>.

2. Department of Defense

a. *National Military Strategy for Cyberspace Operations (2006)*

This classified 54-page document was signed by SecDef in 2006, but was later redacted and released in an unclassified version. The National Military Strategy for Cyberspace Operations (NMS-CO) was one of the first attempts by DOD to describe the cyberspace domain, define cyber threats and vulnerabilities, and provide a strategic framework for governmental action.

The strategy addressed numerous ways to achieve DOD cyberspace goals, one of which was “Partnering with International Coalitions.” It stated, in part, “The U.S. must build and maintain coalitions that are adaptable and capable of evolving throughout and operation. *Integrating coalition partners* early into the planning process reduces operational seams across the coalition and increases the overall success of operations.” (Emphasis added.)⁹⁵

b. *Unified Command Plan (2011)*

Signed by the president, the Unified Command Plan (UCP) is the most strategic, foundational military document. Drafted every two years, the Pentagon adjusts its missions, responsibilities, and geographic boundaries of each Combatant Command based upon each UCP published. Per the current version, U.S. Strategic Command (USSTRATCOM) has overall responsibility for conducting critical cyberspace operations via their sub-unified command, U.S. Cyber Command (USCYBERCOM).⁹⁶

⁹⁵ Sean Lawson, “DOD’s ‘First’ Cyber Strategy Is Neither First, Nor A Strategy,” Forbes, 1 Aug 2011, Accessed 13 Jan 2015, <http://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/>

⁹⁶ U.S. Department of Defense, “Unified Command Plan,” 2011, accessed 14 Jan 2015, <http://www.defense.gov/releases/release.aspx?releaseid=14398>.

c. National Military Strategy (2011)

The unclassified National Military Strategy (NMS) serves as the means for the CJCS to provide “the best military advice”⁹⁷ to the Nation’s leadership, and outlines the ways and means by which the U.S. military advances the Nation’s enduring national interests:

This strategy outlines three broad themes: First, in supporting national efforts to address complex security challenges, the Joint Force’s leadership approach is often as important as the military capabilities we provide. Second, the changing security environment requires the Joint Force to *deepen security relationships with our allies and create opportunities for partnerships with new and diverse groups of actors*. And third, our Joint Force must prepare for an increasingly dynamic and uncertain future in which a full spectrum of military capabilities and attributes will be required to prevent and win our Nation’s wars.

Cyberspace capabilities enable Combatant Commanders to operate effectively across all domains. Strategic Command and Cyber Command will collaborate with U.S. government agencies, nongovernment entities, industry, *and international actors* to develop new cyber norms, capabilities, organizations, and skills. Should a large-scale cyber intrusion or debilitating cyber attack occur, we must provide a broad range of options to ensure our access and use of the cyberspace domain and hold malicious actors accountable. (Emphasis added.)⁹⁸

Finally, “Joint Forces will secure the ‘.mil’ domain, requiring a resilient DOD cyberspace enterprise that employs detection, deterrence, denial, and multi-layered defense.”⁹⁹ (Thus, DOD is chartered to focus on the “.mil” domain, while DHS focuses on the broader “.gov” domain.)

⁹⁷ U.S. Department of Defense, “Chairman’s Corner: 2011 National Military Strategy,” accessed 13 Jan 2015, <http://www.defense.gov/news/newsarticle.aspx?id=62736>.

⁹⁸ Ibid., 10.

⁹⁹ Ibid., 19.

d. CJCS Volume VI Emergency Action Procedures (2012)

Whenever there is a national military emergency, all appropriate military and federal agencies are gathered together on a classified conference call to review the current situation and discuss the way ahead. These conferences are guided by the Emergency Action Procedures of the Chairman of the Joint Chiefs of Staff, Volume VI, “Emergency Conferences.” In the latest version, Commander USCYBERCOM is identified as being the deciding authority for assessing if a “Cyberspace Attack” has occurred, is occurring, or is imminent.¹⁰⁰

e. Joint Publication 3-12, Cyberspace Operations (2013)

As outlined in the unclassified, releasable version, this publication states:

In support of Unified Command Plan-assigned missions, CDRUSSTRATCOM:

- (a) Coordinates with the [intelligence community], [Combatant Commanders], Services, agencies, *and allied partners* to facilitate development of improved cyberspace access to support planning and operations.
- (b) Provides shared [situational awareness] of [cyberspace operations or CO] and [Indications & Warning.]
- (c) Provides military representation to U.S. national agencies, U.S. commercial entities, *and international agencies* for cyberspace matters, as directed. (Emphasis added.)¹⁰¹

¹⁰⁰ U.S. Department of Defense, “CJCS Conferencing Systems,” 3 Feb 2012, accessed 14 Jan 2015, http://dtic.mil/cjcs_directives/cdata/unlimit/3420_01.pdf.

¹⁰¹ U.S. Department of Defense, Joint Publication 3-12R (Releasable), “Cyberspace Operations,” 5 Feb 2013, III-5, accessed 14 Jun 2015, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

This publication discusses cyberspace operations conducted in cooperation with allied nations: “Regardless of what elements are established, *the overlaps between global and theater missions in cyberspace, and the constraints and restraints on personnel conducting CO, necessitate close coordination between the [Combatant Commander], CDRUSSTRATCOM, and other allied and interagency partners for the effective synchronization of CO.*” (Emphasis added.)¹⁰²

Finally, the strategy warns: “Security restrictions may prevent full disclosure of individual CO plans and orders with multinational partners; this may severely hamper cyberspace synchronization efforts. Therefore, the JFC’s staff *should obtain approval for information sharing among partners, and then issue specific guidance on the release of classified U.S. material to the multinational force as early as possible during planning.*” (Emphasis added.)¹⁰³

D. CANADIAN NATIONAL CYBERSPACE GUIDANCE

1. Executive Branch

a. Canada’s Cyber Security Strategy (2010)

This strategy is the Canadian government’s plan for meeting the cyberspace threat, and delivers on the government’s commitment to implement a cyberspace strategy to protect Canada’s digital infrastructure. It acts as a cornerstone of the government’s commitment to keep Canada, including their cyberspace, safe, secure, and prosperous.

b. Action Plan 2010–2015 (2013)

This document outlines the Canadian government’s plan to implement the Cyber Security Strategy and meet the ultimate goal of securing Canada’s cyberspace for the benefit of Canadians and their economy. The Action Plan then outlines thirty specific actions to take, the required deliverables, and the lead agencies involved, all coordinated to meet the three pillars outlined in the Cyber Security Strategy.

¹⁰² Ibid., IV-9.

¹⁰³ Ibid., IV-14.

2. Department of National Defence

a. *Canada First Defence Strategy (2013)*

This strategy sets a detailed road-map for the modernization of the Canadian military forces. Under “Defending North America,” the strategy states, “Given our common defence and security requirements, it is in Canada’s strategic interest to remain a reliable partner in the defence of the continent. Canadian Forces will continue to collaborate with the U.S. counterparts as partners in NORAD...*NORAD is also evolving to meet future threats...*Finally, the two nation’s armed forces will pursue their effective collaboration on operations in North America and abroad.” (Emphasis added.)¹⁰⁴

b. *Canadian Forces Cyber Operations Primer (2014)*

The purpose of this Primer is to describe Cyber Operations from a Canadian Armed Forces (CAF) perspective, and outlines the operational functions in the Cyber environment, those being Command, Sense, Act, Shield, and Sustain. Under the “Sustain” function, the Primer states, “Sustaining the Force requires the CAF to engage in a wide range of multi-national political/military alliances and arrangements (i.e., Five-Eyes, NATO, *NORAD*.)” (Emphasis added.)¹⁰⁵

E. SUMMARY

Over the course of 50 years, NORAD has repeatedly reassessed, redefined, and updated its core operational missions based upon a constantly evolving threat. The NORAD Agreement clearly reflects both Nation’s desire that NORAD be able to adapt and defend against newly evolving military threats which each nation may jointly face:

¹⁰⁴ Canadian Department of National Defence, “Canada First Defence Strategy, accessed 15 Jan 2015, <http://www.forces.gc.ca/en/about/canada-first-defence-strategy.page>.

¹⁰⁵ Canadian Department of National Defence, “Canadian Armed Forces Cyber Operations Primer,” Feb 2014, 6.

MINDFUL that in the years since the first NORAD Agreement was concluded on May 12, 1958, NORAD, as a distinct command, has evolved to address the continuing changes in the nature of the threats to North America and that it will need to *continue to adapt to future shared security interests.* (Emphasis added.)¹⁰⁶

As has been shown, numerous U.S. national strategies recommend working with international organizations to develop international watch-and-warning networks in order to detect and prevent cyber attacks. For example, the Cyberspace Policy Review recommended the U.S. develop international cybersecurity frameworks and partnerships, while the NSS recommended expanding international partnerships regarding network defense and response to cyber attack.

From a U.S. military cyberspace strategy perspective, the NMS-CO identified the need to integrate allies early in the planning process to ensure mission success. One of its three broad themes stressed the need to deepen security relationships with our allies.

Finally, from a Canadian perspective, both Canada's civilian and military strategies mirror these same themes of working with international organizations to develop international watch-and-warning networks in order to detect and prevent cyber attacks. CAF will continue to collaborate with the U.S. counterparts as partners in NORAD as it evolves to meet future threats while pursuing effective collaboration on operations in North America and abroad.

In summary, the U.S. and Canada strategic cyberspace guidance all propose a closer working arrangement between each country as both deal with growing cyberspace threats. These documents significantly inform the discussion regarding NORAD potential new role in cyberspace threat information and attack assessment.

¹⁰⁶ North American Aerospace Defense Command, "NORAD Agreement," accessed 3 Feb 2014, <http://www.norad.mil/AboutNORAD/NORADAgreement.aspx>.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. COURSES OF ACTION DEVELOPMENT

A. METHODOLOGY

The purpose of this chapter is to present potential courses of action (COAs) for NORAD consideration regarding possible roles the Command might play in future military cyber attack warnings. Each of the three selected COAs met all five of the following validity criteria used by the Department of Defense:

- Adequate. Can accomplish the mission within the commander's guidance.
- Feasible. Can accomplish the mission within the established time, space, and resource limitations.
- Acceptable. Must balance cost and risk with advantage gained.
- Distinguishable. Must be sufficiently different from other COAs.
- Complete. Does it answer who, what, where, when, how and why?¹⁰⁷

The author used existing documentation and dialogue with NORAD, USNORTHCOM, USCYBERCOM, and Canadian military cyberspace practitioners. Because much of the cyber mission is currently evolving, it was necessary to extract cyber policy related to NORAD from current joint doctrine and actual cyberspace operations. Formal interviews or surveys were not used.

Numerous COAs were then analyzed and discarded. (Rejected COAs included NORAD developing its own definition of “cyber attack,” outsourcing all NORAD cyber warning functions to USCYBERCOM, and Commander NORAD conducting his own unilateral cyber attack assessments.) Eventually, three reasonable COAs emerged. They were sequentially arranged by increasing levels of responsibility being placed upon NORAD, and were then examined for their specific advantages, disadvantages, and levels of difficulty in their implementation.

¹⁰⁷ U.S. Department of Defense, Joint Publication 5-0, “Joint Operation Planning,” 11 Aug 2011, IV-24 through IV-36, accessed 21 Apr 2015, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

B. COA #1 DESCRIPTION (FULL NORAD CYBER CONFERENCE PARTICIPATION)

1. Definition

Under this COA, NORAD's role would be to fully participate in all cyberspace event conferences in order to increase the Command's internal situational awareness regarding in-progress, military-related cyber events.

2. Discussion

NORAD currently participates in "Cyber Watch Conferences" which provide cyber technicians a standardized venue to discuss and troubleshoot detected system anomalies. However, during advanced "Cyber Event Conferences" and "National Event Conferences," practitioners report Canadian participation is denied approximately 50 percent of the time due to discussions involving non-releasable (US-only) classified cyberspace compartmented information.

Accomplishing this COA eliminates those restrictions, makes classified cyber event information fully available to appropriate Canadian military personnel, and improves NORAD's own cyberspace situational awareness and ability to gauge any associated mission impacts.

3. Advantages

- Allows full cyber event information exchange to both U.S. and Canadian personnel assigned to NORAD.
- Enables NORAD full situational awareness regarding cyber events that might affect the NORAD warning and control missions.
- Uses existing technical conference procedures.
- Does not change existing relationships with USCYBERCOM.
- Does not require a change in the NORAD Agreement and/or Terms of Reference negotiated between the U.S. and Canada.

4. Disadvantages and Proposed Solutions

- Some classified cyberspace threat information and technical “tactics, techniques, and procedures” (TTPs) are not currently releasable to Canadian personnel. (Change DOD classification guidance to allow Canadians full access to cyberspace threat information and TTPs.)
- NORAD regional headquarters currently must drop off threat conferences during classified discussions. (Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.)
- Modifies existing conference checklist procedures. (Modify cyberspace conference checklists to reflect full NORAD participation.)

C. COA #2 DESCRIPTION (NORAD ALL-DOMAIN WARNING PRODUCTION)

1. Definition

Under this COA, NORAD’s role would be to fuse applicable North America military-related cyber event information with current NORAD aerospace and maritime operational information to produce all-domain warnings to the U.S. and Canadian governments.

2. Discussion

Assuming the issue of releasing classified cyber event information to NORAD Canadians was successfully resolved (proposed in COA #1), this COA directs NORAD to fuse military cyber event information with current aerospace and maritime warning information to produce timely, all-domain warnings to the U.S. and Canadian governments using existing NORAD binational military relationships and established warning processes. This COA would allow Canadian cyber forces to become involved in the NORAD notification process. As technical cyber event information would initially be analyzed by USCYBERCOM, then provided to NORAD for further amalgamation, there would be no change to the existing relationships between the two commands.

3. Advantages

- Allows full cyber event information exchange to both U.S. and Canadian personnel assigned to NORAD.
- Enables NORAD full situational awareness regarding cyber events that might affect the NORAD warning and control missions.
- Uses existing technical conference procedures.
- Does not change existing relationships with USCYBERCOM.
- Directs NORAD to fuse military cyber event information with current aerospace and maritime warning information to produce an all-domain characterization.
- Uses proven, legacy NORAD binational relationships and procedures to provide immediate all-domain warning updates to both the U.S. and Canadian military command structures.

4. Disadvantages and Proposed Solutions

- Some classified cyberspace threat information and technical TTPs are not currently releasable to Canadian personnel. (Change DOD classification guidance to allow Canadians full access to cyberspace threat information and technical TTPs.)
- NORAD regional headquarters currently must drop off threat conferences during classified SCI discussions. (Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.)
- Modifies existing conference checklist procedures. (Modify cyberspace conference checklists to reflect NORAD fusing and dissemination of all-domain warning updates to both the U.S. and Canada.)
- Requires training NORAD personnel to fuse and disseminate all-domain warning updates. (Build new training program for NORAD personnel to fuse and disseminate all-domain warning updates.)

- Requires negotiating new cyberspace defense and response policies between the U.S. and Canada. (Negotiate new cyberspace defense and response policies between the U.S. and Canada, if required.)
- Requires a change in NORAD Agreement and/or Terms of Reference between both Governments. (Negotiate change to NORAD Agreement and/or Terms of References between the U.S. and Canada, if required.)

D. COA #3 DESCRIPTION (JOINT NORAD + USCYBERCOM CYBER ATTACK ASSESSMENT)

1. Definition

Under this COA, NORAD's role would involve CDRNORAD and CDRUSCYBERCOM to conducting a combined formal cyber attack assessment, if such an attack was believed to be in progress.

2. Discussion

Again, assuming the releasability of classified cyber event information (proposed in COA #1) was successfully accomplished, this COA would require joint concurrence regarding a cyber attack assessment. While CDRUSCYBERCOM understands the technical cyberspace issues involved during a cyber attack, CDRNORAD has the operational responsibility to provide aerospace and maritime attack warning for North America to the civilian military leadership of both Nations. Providing a joint assessment would strengthen the validity of such an evaluation.

3. Advantages

- Allows full cyber event information exchange to both U.S. and Canadian personnel assigned to NORAD.
- Enables NORAD full situational awareness regarding cyber events that might affect the NORAD warning and control missions.
- Uses existing technical conference procedures.

- Leverages USCYBERCOM’s global cyberspace visibility, technical infrastructure, and cyberspace expertise to accomplish an official cyber attack assessment.
- Leverages NORAD’s visibility on current air defense operations and aerospace/maritime warning expertise to ascertain any effects on NORAD operations.

4. Disadvantages and Proposed Solutions

- Some classified cyberspace threat information and technical TTPs are not currently releasable to Canadian personnel. (Change DOD classification guidance to allow Canadians full access to cyberspace threat information and technical TTPs.)
- NORAD regional headquarters currently must drop off threat conferences during classified discussions. (Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.)
- Modifies existing conference checklist procedures. (Modify cyberspace conference checklists to reflect joint CDRUSCYBERCOM/CDRNORAD cyber attack assessment.)
- Requires training NORAD General Officers for new cyber attack assessment coordination responsibility. (Build new training program for NORAD General Officer joint cyber attack assessment responsibility.)
- Changes existing relationships with USCYBERCOM. (Negotiate new command arrangements agreement between NORAD and USCYBERCOM.)
- Requires negotiating new cyberspace defense and response policies between the U.S. and Canada. (Negotiate new cyberspace defense and response policies between the U.S. and Canada, if required.)
- Requires changing the NORAD Agreement and/or Terms of References. (Negotiate change to NORAD Agreement and/or Terms of Reference, if required.)

E. SUMMARY

This chapter identified three general COAs regarding possible roles NORAD might play in future military cyber attack warning situations. Each proposed COA was initially analyzed to ensure it met specific validity criteria (e.g., adequate, feasible, acceptable, distinguishable, and complete.) COAs were then arranged by increasing levels of responsibility being placed upon NORAD. Each COA was then examined for specific advantages. Finally, each COA was then examined for specific disadvantages, disadvantages, and possible solutions for implementation and subsequent COA analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

V. COURSES OF ACTION ANALYSIS

A. METHODOLOGY

Three general courses of action (COAs) were identified regarding possible roles NORAD might play in future military cyber attack warning. These COAs were arranged by increasing levels of responsibilities being placed upon NORAD. Advantages were listed to allow the reader a broad appreciation of the operational benefits each COA might offer.

Next, in order to gauge to what extent a proposed COA was practical to implement, disadvantages were listed with corresponding proposed solutions. These proposed solutions were then standardized across all COAs to allow for uniform comparison.¹⁰⁸

Using inputs from cyberspace subject matter experts, each proposed solution was then weighted for its general difficulty in implementation, with a score of either:

- “1” (Routine; requires normal NORAD internal staff actions.)
- “2” (Challenging; requires detailed, U.S. government-wide staff actions.)
- “3” (Difficult; requires politically sensitive binational staff actions.)

Finally, all weighted factors were then summed to present a total score for consideration. The COA which presented the greatest apparent advantages and the lowest disadvantages score was presumed to be the best COA for NORAD to pursue.

Overall, this methodology (while not strictly scientific) provides the reader a general measure of the effectiveness and cost of implementation for each proposed COA. (Before any COA might be adopted, it is suggested a full military COA analysis be conducted, to include surveys and/or interviews with cyberspace practitioners.)

This chapter concludes with a summary table identifying all COAs, their proposed solutions and weights, and their specific scorings.

¹⁰⁸ Morgan D. Jones, *The Thinker’s Toolkit*, New York, NY, Crown Publishing Group, 30 Jun 1998, chapters 4 and 10.

B. COA #1 ANALYSIS (FULL NORAD CYBER CONFERENCE PARTICIPATION)

1. Advantages, Disadvantages and Weighted Scoring

- Allows full cyber event information exchange to both U.S. and Canadian personnel assigned to NORAD.
- Enables NORAD full situational awareness regarding cyber events that might affect the NORAD warning and control missions.
- Uses existing technical conference procedures.
- Does not change existing relationships with USCYBERCOM.
- Does not require a change in the NORAD Agreement and/or Terms of Reference negotiated between the U.S. and Canada.

DISADVANTAGES	SOLUTIONS	WEIGHT
Modifies existing conference checklist procedures.	Modify cyberspace conference checklists to reflect full NORAD participation.	1
Some classified cyberspace threat information and technical TTPs are not currently releasable to Canadian personnel.	Change DOD classification guidance to allow Canadians full access to cyberspace threat information and technical TTPs.	2
NORAD regional headquarters currently must drop off threat conferences during classified discussions.	Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.	2
	SCORE	5

Table 2. COA #1 Scoring Summary.

2. COA #1 Synopsis

COA #1 is a promising first step. (In fact, NORAD and USNORTHCOM staffs are currently attempting to obtain DOD approval to release classified technical cyberspace information to Canadian NORAD members for the very reasons outlined in the COA rationale.)

Overall, this would seem to be a realistic, achievable COA that offers significant improvement in NORAD cyber attack situational awareness and operational effectiveness at a cost of only an administrative change in DOD information classification policy.

Releasing classified cyberspace information to all NORAD personnel, and allowing NORAD regional headquarters to remain on cyber event conferences, also mirrors current U.S. national policies which repeatedly highlight the need for greater U.S. cooperation and information sharing with our international allies.

This COA is also in keeping with the spirit of the NORAD agreement, where the Command remains in the situational awareness business, yet can be responsive to any cyberspace actions being undertaken by USCYBERCOM.

Under this COA, existing classified cyber event conferences would continue as normal. However, updated internal NORAD operational checklists would be required to fully capitalize on new cyber attack warning information now being available to NORAD personnel from such cyberspace conference attendance.

After reviewing the advantages, disadvantages and potential solutions for implementing this COA, a weighted implementation score of “5” would seem to indicate few major roadblocks to overcome.

Overall, while requiring several “challenging” staff actions through DOD to accomplish the desired releasability goal, this COA would enable greater information exchange between allies, would provide greater cyberspace situational awareness to NORAD, and would help Commander NORAD make more knowledgeable assessments regarding any potential attack upon North America.

C. COA #2 ANALYSIS (NORAD ALL-DOMAIN WARNING PRODUCTION)

1. Advantages, Disadvantages and Weighted Scoring

- Allows full cyber event information exchange to both U.S. and Canadian personnel assigned to NORAD.
- Enables NORAD full situational awareness regarding cyber events that might affect the NORAD warning and control missions.
- Uses existing technical conference procedures.
- Does not change existing relationships with USCYBERCOM.
- Directs NORAD to fuse military cyber event information with current aerospace and maritime warning information to produce an all-domain characterization.
- Uses proven, legacy NORAD binational relationships and warning procedures to provide immediate all-domain warning updates to both the U.S. and Canadian military command structures.

DISADVANTAGES	SOLUTIONS	WEIGHT
Modifies existing conference checklist procedures.	Modify cyberspace conference checklists to reflect NORAD fusing and dissemination of all-domain warning updates to both the U.S. and Canada.	1
Some classified cyberspace threat information and technical TTPs are not currently releasable to Canadian personnel.	Change DOD classification guidance to allow Canadians full access to cyberspace threat information and technical TTPs.	2
NORAD regional headquarters currently must drop off threat conferences during classified discussions.	Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.	2
Requires training NORAD personnel to fuse and disseminate all-domain warning updates.	Build new training program for NORAD personnel to fuse and disseminate all-domain warning updates.	2

Requires negotiating new cyberspace defense and response policies between the U.S. and Canada.	Negotiate new cyberspace defense and response policies between the U.S. and Canada, if required.	3
Requires a change in the NORAD Agreement and/or Terms of Reference.	Negotiate change to NORAD Agreement or Terms of Reference, if required.	3
	SCORE	13

Table 3. COA #2 Scoring Summary.

2. COA #2 Synopsis

COA #2 proposes a much more active role for NORAD, assuming the issue regarding the releasability of classified cyber event information to Canadian personnel (proposed under COA #1) has been successfully resolved. It directs the Command to fuse military cyber event information with existing aerospace and maritime warning information to produce timely, all-domain warnings to U.S. and Canada national civilian leadership using current NORAD binational military relationships and established warning processes.

While USCYBERCOM currently provides specific cyber event updates directly to military command centers, having NORAD produce a broader, all-domain warning products to both the U.S. and Canada would help both nations have a better appreciation the effect a cyber event might have had on North American defenses.

Under this COA, existing classified cyber event conferences continue as normal and capitalize on information now being fully available to all NORAD personnel. Updated internal operational checklists would be required to reflect NORAD fusing and dissemination of all-domain warnings to both Nations. Also, a new training program would have to be built to train NORAD personnel on producing and disseminating all-domain warning products.

As cyber event formation would initially be analyzed by USCYBERCOM, then provided to NORAD for further consideration, there would be no change to the existing relationships between the two commands.

Also, because this would be a major change to NORAD's legacy missions and processes, new cyberspace defense and response policies might have to be negotiated between the U.S. and Canada to ensure NORAD has the correct mission authority. Following such binational negotiations, the NORAD Agreement and /or Terms of References would also need updating through international staffing channels.

After reviewing the advantages, disadvantages and potential solutions for implementing this COA, a weighted implementation score of "13" would seem to indicate several major roadblocks to overcome, mostly in the need to negotiate new international agreements between the U.S. and Canada.

Overall, while requiring both "challenging" and "difficult" staff actions both within DOD and internationally with Canada, this COA harnesses proven NORAD binational relationships and warning procedures to provide all-domain warning updates to both nations.

D. COA #3 ANALYSIS (JOINT NORAD + USCYBERCOM CYBER ATTACK ASSESSMENT)

1. Advantages, Disadvantages and Weighted Scoring

- Allows full cyber event information exchange to both U.S. and Canadian personnel assigned to NORAD.
- Enables NORAD full situational awareness regarding cyber events that might affect the NORAD warning and control missions.
- Uses existing technical conference procedures.
- Leverages USCYBERCOM's global cyberspace visibility, technical infrastructure, and cyberspace expertise to accomplish an official cyber attack assessment.
- Leverages NORAD's visibility on current air defense operations and aerospace/maritime warning expertise to ascertain any effects on NORAD operations.

DISADVANTAGES	SOLUTIONS	WEIGHT
Modifies existing conference checklist procedures.	Modify cyberspace conference checklists to reflect joint CDRUSCYBERCOM / CDRNORAD cyber attack assessment.	1
Some classified cyberspace threat information and technical TTPs are not currently releasable to Canadian personnel.	Change DOD classification guidance to allow Canadians full access to cyberspace threat information and technical TTPs.	2
NORAD regional headquarters currently must drop off threat conferences during classified discussions.	Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.	2
Requires training NORAD General Officers for new cyber attack assessment coordination responsibility.	Build new training program for NORAD General Officer joint cyber attack assessment responsibility.	2
Changes existing relationships with USCYBERCOM.	Negotiate new command arrangements agreement between NORAD and USCYBERCOM.	2
Requires negotiating new cyberspace defense and response policies between the U.S. and Canada.	Negotiate new cyberspace defense and response policies between the U.S. and Canada, if required.	3
Requires changing the NORAD Agreement and /or Terms of Reference between both governments.	Negotiate change to NORAD Agreement and/or Terms of Reference between both governments, if required.	3
	SCORE	15

Table 4. COA #3 Scoring Summary.

2. COA #3 Synopsis

COA #3 is the most active NORAD option. Again, assuming the release of classified cyber event information to Canadian personnel (proposed under COA #1) has been successfully accomplished, this COA proposes a major change in current U.S. cyber attack assessment procedures.

While USCYBERCOM has strong technical understanding and global visibility of cyberspace activities, they often lack detailed insight into current operations being conducted by global combatant commands. Under this COA, this deficit would be alleviated for North American air defense operations by directing NORAD to jointly participate in all North American-related cyber attack assessments. Commander NORAD would bring an awareness of on-going continental air defense operations, would provide essential operational expertise when adjudicating proposed cyberspace attack assessments, and could evaluate what effects any proposed follow-on cyberspace actions might have on current NORAD operations.

Some staffs have argued this COA is not required, as Commander USNORTHCOM (dual-hatted as Commander NORAD) already has the authority to declare a “Domestic Attack Assessment” if he judges the U.S. is under attack. Already having this authority would seem to obviate the need for him to assume an additional cyber attack assessment responsibility. However, his role as Commander USNORTHCOM does not specifically involve cyberspace operations, only involves U.S. military responsibilities, and does not involve notifications to the Canadian government which automatically occur within the binational NORAD structure.

Another concern voiced is allowing another commander to participate in the cyber attack assessment process. One could argue if Commander NORAD needs to participate in North American-related cyber events, then should not Commander European Command participate in European-related cyber events, or Commander Pacific Command participate in cyber events occurring in Asia? Once the USCYBERCOM assessment process is opened to other geographic combatant commanders, does not this become a very slippery slope?

Under this COA, existing classified cyber event conferences continue as normal. Updated internal NORAD operational checklists would be required to reflect joint CDRCYBERCOM and CDRNORAD participation in all cyber attack assessments. Also, a new training program would have to be built to train NORAD General Officers on their new joint assessment responsibility.

Also, if this COA were to be implemented, a new “Command Arrangements Agreement” between NORAD and USCYBERCOM would need to be negotiated to clearly outline the new cyber attack assessment responsibilities of each commander.

Further, because this would be a major change to NORAD’s legacy missions and processes, new cyberspace defense and response policies might have to be negotiated between the U.S. and Canada to ensure NORAD has the correct mission authority. Following such binational negotiations, the NORAD Agreement and /or Terms of References would also need updating through international staffing channels.

After reviewing the advantages, disadvantages and potential solutions for implementing this COA, a weighted implementation score of “15” would seem to indicate several major roadblocks to overcome, mostly in the need to negotiate international agreements between the U.S. and Canada, and new command agreements between NORAD and USCYBERCOM.

Overall, while requiring both “challenging” and “difficult” staff actions both within DOD and internationally with Canada, this COA combines the advantages which both NORAD and USCYBERCOM offer to the cyber attack assessment process.

E. COA ANALYSIS COMPARISON

Using inputs from cyberspace subject matter experts, each COA proposed implementation solutions which were weighted using an increasing score of either:

- “1” (Routine; requires normal NORAD internal staff actions.)
- “2” (Challenging; requires detailed, U.S. government-wide staff actions.)
- “3” (Difficult; requires politically sensitive binational staff actions.)

All weighted factors were then summed to present a total COA score for consideration. The COA which presented the greatest apparent advantages and the lowest disadvantages score was presumed to be the best COA for NORAD to pursue.

Table 5 summarizes all three COAs, their proposed solutions and implementation weights, and their specific total scorings:

Proposed Solutions	Weight	COA 1 Full NORAD Cyber Conference Participation	COA 2 NORAD All-Domain Warning Production	COA 3 Joint NORAD + USCYBERCOM Cyber Attack Assessment
Modify cyberspace conference checklists to reflect full NORAD participation.	1	1		
Modify cyberspace conference checklists to reflect NORAD fusing and dissemination of all-domain warnings to both the U.S. and Canada.	1		1	
Modify cyberspace conference checklists to reflect joint CDRUSCYBERCO M / CDRNORAD cyber attack assessment.	1			1
Change DOD classification guidance to allow Canadians full access to cyberspace threat information and technical TPPs.	2	2	2	2

Change DOD conference procedures to allow NORAD regional headquarters to remain on cyber event conferences during classified discussions.	2	2	2	2
Build new training program for NORAD personnel to fuse and disseminate all-domain warning updates.	2		2	
Build new training program for NORAD General Officer joint cyber attack assessment responsibility.	2			2
Negotiate new command arrangements agreement between NORAD and USCYBERCOM.	2			2
Negotiate new cyberspace defense and response policies between the U.S. and Canada, if required.	3		3	3
Change NORAD Agreement and/or Terms of Reference, if required.	3		3	3
SCORES		5	13	15

Table 5. COA Analysis Summary.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. FINDINGS AND RECOMMENDATIONS

A. FINDINGS

This thesis began with an examination of NORAD's history of evolving to meet new military defense challenges. It also examined cyber warfare components and evolving definitions, key U.S. and Canadian military cyber organizations, and current cyberspace national event conferences. With the dramatic increase in world-wide cyberspace events, it was noted NORAD has begun examining its own potential role in this new operational domain.

This thesis then examined current NORAD, U.S. and Canadian strategic guidance relating to cyberspace operations. Both the NORAD Agreement clearly reflect both Nation's desire that NORAD be able to adapt and defend against newly evolving military threats which each nation may jointly face. Likewise, numerous U.S. government strategies recommend working with international organizations to develop watch-and-warning networks in order to detect and prevent cyber attacks. Further, U.S. military cyberspace policies identify the need to integrate coalition partners early into planning processes and thus increase the overall success of combined operations. Finally, from a Canadian perspective, both their civilian and military strategies mirror these same themes of working with international organizations to develop international watch-and-warning networks in order to detect and prevent cyber attacks. In summary, both U.S. and Canada strategic cyberspace guidance propose a closer working arrangement between each country as a means of dealing with growing cyberspace threats. These documents significantly inform the discussion regarding NORAD potential new role in cyberspace threat information and attack assessment.

With this policy background in mind, three courses of action (COAs) were eventually developed regarding possible roles NORAD might play in future military cyber attack warning situations. Each proposed COA was initially analyzed to ensure it met specific validity criteria. They were then examined for specific advantages, disadvantages, and possible solutions (each generally weighted for implementation).

COA #1 proposes NORAD advocate for full national cyberspace conference participation. Overall, this would seem to be a realistic, achievable first step that offers significant improvement in NORAD cyber attack situational awareness and improved operational responsiveness requiring only a change in DOD information classification policy. Allowing NORAD Canadian personnel to fully participate in cyber event conferences also mirrors current U.S. national policies which repeatedly highlight the need for greater U.S. and Canadian cooperation and information sharing with between allies. After reviewing the advantages, disadvantages and potential solutions for implementing this COA, a weighted implementation score of “5” seems to indicate few major roadblocks to overcome.

In general, while requiring several “challenging” staff actions through DOD to accomplish the desired releasability goal, this COA would enable greater information exchange between allies, would provide greater cyberspace situational awareness to NORAD, and would help Commander NORAD make more knowledgeable assessments regarding any potential attack upon North America.

COA #2 proposes NORAD produce all-domain warnings using its legacy binational military relationships and warning processes. This proposes a much more active role for NORAD, necessitating a new program to train NORAD personnel on producing all-domain warning products. While USCYBERCOM would continue to provide cyber event updates directly to military command centers, NORAD would produce broader, all-domain warnings to help both nations have a better appreciation the effect cyber events might have on North American defenses. COA analysis revealed a solution score of “13,” indicating several major roadblocks to overcome, mostly in the need to negotiate new international agreements between the U.S. and Canada.

Overall, while requiring “challenging” and “difficult” staff actions within DOD and internationally with Canada, this COA harnesses proven NORAD binational relationships and warning procedures to provide all-domain warnings to both nations.

Finally, COA #3 proposes a joint NORAD and USCYBERCOM cyber attack assessment concept. This would be a major change for both NORAD and the U.S. cyberspace community, as well. This COA argues while USCYBERCOM has strong technical understanding and global visibility of cyberspace activities, they often lack detailed insight into current operations being conducted by global combatant commands. Under this COA, this deficit would be alleviated for North American air defense operations by directing NORAD to jointly participate in all North American-related cyber attack assessments.

However, a strong argument against this COA concerns opening up the attack assessment role to all geographic commanders. Thus, it could be argued if Commander NORAD needs to participate in North American-related cyber events, then Commander European Command should participate in European-related cyber events, and Commander Pacific Command should participate in cyber events occurring in Asia.

Further, as this would be a major change to NORAD's legacy missions, new cyberspace defense and response policies would need to be negotiated between the U.S. and Canada to ensure NORAD has correct mission authority. Following such binational negotiations, the NORAD Agreement and Terms of References would also need updating through international staffing channels. After reviewing the advantages, disadvantages and potential solutions for implementing this COA, a weighted score of "15" indicates several major roadblocks to be overcome, to include negotiating new international agreements between the U.S. and Canada, and the need to develop a new NORAD General Officer cyber attack assessment training program.

Overall, while requiring both "challenging" and "difficult" staff actions both within DOD and internationally with Canada, this COA combines the advantages which NORAD and USCYBERCOM both offer to the cyber attack assessment process.

B. RECOMMENDATIONS

As the COAs were being developed, it became apparent they were not mutually exclusive, but in fact all of these COAs could potentially be adopted sequentially over the course of several years.

COA #1 offers a major improvement in cyber situational awareness at little implementation cost. The difficulty will be in convincing DOD the need to change its administrative policies regarding the sharing of classified cyberspace operational information with Canadian military personnel. This would not be a trivial endeavor. However, this thesis has highlighted numerous strategic policies which emphasize the need to share this type of information with international partners, and NORAD Canadians are clearly one of the longest and most enduring allies to the U.S. Overall, this COA would seem to be the easiest to implement while significantly improving NORAD's cyber situational awareness.

Later, as cyberspace information sharing with Canadians becomes routine, NORAD could reevaluate whether it is militarily desirable to pursue COA #2. This would be a subjective evaluation by the NORAD, USCYBERCOM, and other cyberspace information users to determine if there was value added in NORAD producing all-domain fused warnings. While COA analysis shows this to involve both "challenging" and "difficult" staff actions, a broader question might be "is there a real customer need?"

Finally, COA #3 may be militarily undesirable. Having Commander NORAD directly involved with North American cyber attack assessments seemed reasonable, but COA analysis showed many roadblocks to success. Further, the "challenging" task of negotiating new CAAs between NORAD and USCYBERCOM might then generate the need to develop similar CAAs between USCYBERCOM and USEUCOM, USPACOM, etc. This greatly expands the overall impact of this COA, probably making this policy option "a bridge too far."

In conclusion, with global cyber attacks on the rise, it seems reasonable NORAD should explore potential new roles for cyber attack warning. This thesis recommends that the NORAD staff consider COA #1 first.

LIST OF REFERENCES

- “2014: Piracy, Terrorism and Direct Maritime Threats.” *The Maritime Executive*, 14 Mar 2014. <http://www.maritime-executive.com/article/2014-Piracy-Terrorism--Diverse-Maritime-Threats-2014-03-14/>.
- “About USNORTHCOM.” U.S. Northern Command, Peterson Air Force Base, Colorado Springs, CO. 3 Apr 2015. <http://www.northcom.mil/AboutUSNORTHCOM.aspx>.
- “At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.” *National Academy of Science*, 2014. http://www.nap.edu/openbook.php?record_id=18749.
- “BPG Final Report on Canada and the U.S. (CANUS) Enhanced Military Cooperation.” NORAD and USNORTHCOM. 13 March 2006.
- “Brief History of NORAD.” North American Aerospace Defense Command History Office, Peterson Air Force Base, Colorado Springs, CO.
- “Canada First Defence Strategy.” Canadian Department of National Defence. <http://www.forces.gc.ca/en/about/canada-first-defence-strategy.page>.
- “Canadian Armed Forces Cyber Operations Primer.” Canadian Department of National Defence.
- “Canadian Joint Operations Command.” Canadian Department of National Defence. <http://www.forces.gc.ca/en/about-org-structure/canadian-joint-operations-command.page>.
- “Chairman’s Corner: 2011 National Military Strategy.” U.S. Department of Defense. <http://www.defense.gov/news/newsarticle.aspx?id=62736>.
- “Chief of the Defence Staff.” Canadian Department of National Defence. <http://www.forces.gc.ca/en/about-org-structure/chief-of-defence-staff.page>.
- “CJCS Conferencing Systems.” U.S. Department of Defense. http://dtic.mil/cjcs_directives/cdata/unlimit/3420_01.pdf.
- Clayton, Mark. “Presidential Cyberwar Directive Gives Pentagon Long-Awaited Marching Orders.” *Christian Science Monitor*, 10 Jun 2013. <http://www.csmonitor.com/USA/Military/2013/0610/Presidential-cyberwar-directive-gives-Pentagon-long-awaited-marching-orders-video>
- “Comprehensive National Cybersecurity Initiative.” The White House. <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>.

“Cruise Missiles.” Federation of American Scientists, 3 Apr 2015. <http://fas.org/nuke/intro/cm/index.html>.

“Cyber Attacks on South Korean Nuclear Power Operator Continue.” *The Guardian*, 28 Dec 2014. <http://www.theguardian.com/world/2014/dec/28/cyber-attacks-south-korean-nuclear-power-operator>.

“Cyberspace Policy Review.” U.S. Department of Homeland Security. <http://www.dhs.gov/publication/2009-cyberspace-policy-review>.

Day, Paul. *Cyberattack*. London, UK, Carlton Publishing Group, 2013.

“Definition of Aggression.” United Nations General Assembly Resolution 3314 (XXIX), Article 1, 14 Dec, 1974. <http://www.un-documents.net/a29r3314.htm>.

Department of the Army, Field Manual 3–38, “Cyber Electromagnetic Activities,” Feb 2014. <http://fas.org/irp/doddir/army/fm3-38.pdf>.

“Evaluating Feasibility of Creating a NORAD-like Organization for the Maritime Environment.” U.S. Department of Defense.

“Fact Sheet: Department of Defense Cyber Strategy.” Department of Defense. April 2015. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf

“Fact Sheet of Presidential Policy Directive 20.” Federation of American Scientists. <http://fas.org/irp/offdocs/ppd/ppd-20-fs.pdf>.

“Infrared Satellites.” U.S. Air Force Factsheet, 19 Dec 2014. <http://www.lasangeles.af.mil/library/factsheets/factsheet.asp?id=20144>.

“Iran’s Support for Terrorism Worldwide.” U.S. House Committee on Foreign Affairs, Joint Subcommittee Hearing. 4 Mar 2014. <http://docs.house.gov/meetings/FA/FA13/20140304/101832/HHRG-113-FA13-20140304-SD001.pdf>.

Jones, Morgan D. *The Thinker’s Toolkit*. New York, NY: Crown Publishing Group, 1998.

Lah, Kyung, and Greg Botelho. “Watch Out World: North Korea Deep Into Cyber Warfare, Defector Says.” *Cable News Network*, 18 Dec 2014. <http://www.cnn.com/2014/12/18/world/asia/north-korea-hacker-network/index.html>.

“Launching the U.S. International Strategy for Cyberspace.” The White House. <http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace>.

Lawson, Sean. "DOD's 'First' Cyber Strategy Is Neither First, Nor a Strategy." *Forbes*, 1 Aug 2011. <http://www.forbes.com/sites/seanlawson/2011/08/01/dods-first-cyber-strategy-is-neither-first-nor-a-strategy/>

"Mission and Priorities." U.S. Strategic Command. <http://www.stratcom.mil/mission/>

"NORAD Agreement." U.S. Department of State. <http://www.state.gov/documents/organization/69727.pdf>.

NORAD and USNORTHCOM. Position Paper #SJS 04–00759. North American Aerospace Defense Command, Peterson Air Force Base, Colorado Springs, CO. 18 March 2004.

"NORAD Strategic Review (S//RELCAN)." North American Aerospace Defense Command, Peterson Air Force Base, Colorado Springs, CO.

"National Security Strategy." The White House. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

"National Strategy to Secure Cyberspace." U.S. Department of Homeland Security. <http://www.dhs.gov/national-strategy-secure-cyberspace>.

NATO Wales Summit Declaration. 5 Sep 2014. <http://www.cfr.org/nato/wales-summit-declaration/p33394>.

"Organizational Structure." Canadian Department of National Defence. <http://www.forces.gc.ca/en/about-org-structure/index.page>.

Paganini, Pierluigi. "APT28: Fireeye Uncovered a Russian Cyber Espionage Campaign." *Security Affairs*, 29 Oct 2014. <http://securityaffairs.co/wordpress/29683/intelligence/apt28-fireeye-russian-espionage.html>.

Page, Tom. "Alaskan DEW Line Sites." *Radomes, Inc.*, 20 Apr 2015. <http://www.radomes.org/museum/alaskadew.php>.

———. "BMEWS Site 1, Under Construction - 1958–1960." *Radomes, Inc.*, 19 Feb 2014. <http://radomes.org/museum/documents/BMEWSSite1ThuleGL1958-60construction.html>.

Park, Ju-Min, and James Pearson. "In North Korea, Hackers Are a Handpicked, Pampered Elite." *Reuters*, 5 Dec 2014. <http://www.reuters.com/article/2014/12/05/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205>.

Pike, John. "Ballistic Missile Early Warning System (BMEWS)." Global Security Organization. 19 Feb 2014. <http://www.globalsecurity.org/space/systems/bmews.htm>.

- Proc, Jerry. "Radio Communications and Signals Intelligence in the Royal Canadian Navy, CFS Leitrim." <http://jproc.ca/rrp/leitrim.html>.
- Rid, Thomas, and Peter McBurney." Cyber-Weapons." *The Rusi Journal*, Feb/Mar 2012. https://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf.
- "Russia Preparing New Cyber Warfare Branch, Military Officials Say." *Softpedia*, 17 Dec 2014. <http://news.softpedia.com/news/Russia-Preparing-New-Cyber-Warfare-Branch-Military-Official-Says-376807.shtml>
- "Space-Based Early Warning: From MIDAS to DSP to SBIRS." National Security Archive. 8 Jan 2013. <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB235/20130108.html>.
- Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, UK: University Press, 2013.
- Schmidt, Michael, and David Sanger. "5 in China Army Face U.S. Charges of Cyberattacks." *New York Times*, 19 May 2014. <http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberespionage.html?r=0>.
- Shafa, Lt Col Eric."Iran's Emergence as Cyber Power." *Strategic Studies Institute*, 19 Aug 2014. <http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20#e11>.
- Stavridis, James. "Incoming: What is a Cyber Attack?" *Signals*, 1 Jan 2015. <http://www.afcea.org/content/?q=node/13832>.
- Sublette, Carey. "The Soviet Nuclear Weapons Program." *The Nuclear Weapons Archive*, 12 December 2007. <http://nuclearweaponarchive.org/Russia/Sovwpnprog.html>.
- "USNORTHCOM Statement." U.S. House of Representatives, Armed Services Committee, 3 Apr 2015. <http://docs.house.gov/meetings/AS/AS00/20130320/100395/HHRG-113-AS00-Wstate-JacobyG-20130320.pdf>.
- "U.S. Cyber Command." U.S. Strategic Command. http://www.stratcom.mil/factsheets/2/Cyber_Command/.
- U.S. Department of Defense. "About the Joint Chiefs of Staff." <http://www.jcs.mil/About.aspx>.
- . "Emergency Action Procedures of the Chairman of the Joint Chiefs of Staff, Volume VI, Emergency Conferences (U)." Arlington County, VA: Department of Defense.

- . Joint Publication 3–12R (Releasable), “Cyberspace Operations,” 5 Feb 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
- . Joint Publication 5–0, “Joint Operation Planning,” 11 Aug 2011. http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.
- . “Organization of the Department of Defense.” <http://odam.defense.gov/OMP/Functions/OrganizationalPortfolios/OrganizationandFunctionsGuidebook.aspx>.
- . “Unified Command Plan.” <http://www.defense.gov/releases/release.aspx?releaseid=14398>.
- Weisgerber, Marcus. “Interview: General Charles Jacoby.” *Defense News*, 19 Jul 2014. <http://www.defensenews.com/article/20140719/DEFREG02/307190018/Interview-Gen-Charles-Jacoby>.
- “Worldwide Threat Assessment of the U.S. Intelligence Community.” U.S. Senate Select Committee on Intelligence. 24 Jan 2014. <http://www.intelligence.senate.gov/140129/clapper.pdf>.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, VA 22060
2. Dudley Knox Library
Naval Postgraduate School
Monterey, CA 93943